MÓDULO DE:

INTRODUÇÃO ÀS REDES DE COMPUTADORES

AUTORIA:

Ing. M.Sc./D.Sc. ANIBAL D. A. MIRANDA

Apresentação

Familiarização do aluno com as diversas técnicas de conectividade entre computadores, criando redes de tamanhos diferentes ,assim como, entender a importância dos protocolos de comunicações para um correto funcionamento desses sistemas interligados de redes.

Objetivo

O histórico, finalidades, formas de transmissão, conceitos básicos de telecomunicações, protocolos, meios de transmissão, topologias, equipamentos, conceitos de segurança em redes, arquitetura de redes e tecnologias de redes.

Ementa

Conceitos gerais; sistemas operacionais de rede; princípios de telecomunicações; redes de computadores; topologia de redes; cabeamento de rede; padrões meios de redes; modelo TCP/IP; dispositivos de redes; gerenciamento de redes; servidores de rede; tecnologias de redes; segurança de redes; Internet; intranet; extranet.

Sobre o Autor

Engenheiro eletrônico especializado nas áreas de Teleinformática e Telecomunicações.

Mestrado e Doutorado outorgados pelo Instituto Tecnológico de Aeronáutica (ITA) em 1998 e 2004 respectivamente.

A Tese de Mestrado rendeu o Primeiro premio "Comandante Quandt de Telecomunicações" na TELEXPO de São Paulo em 1999. Categoria: Trabalhos Técnicos.

Autor de softwares na área de engenharia de tráfego, principalmente para medir, analisar e emular o comportamento agregado de pacotes IP.

Autor de vários artigos técnicos apresentados em importantes congressos a nível nacional e internacional.

Boa experiência no estudo, análise, dimensionamento e implementação de projetos na área de Teleinformática.

SUMÁRIO

UNIDADE 1

Objetivo: Entender a importância dos sistemas de comunicações à distância.

Conceitos Gerais

Introdução

Define-se como sistema o conjunto de objetos ou pessoas intrinsecamente relacionados entre si para um determinado fim ou propósito. Nesse sentido, uma rede de comunicações é um sistema de dispositivos eletrônicos, objetos e pessoas intrinsecamente conectadas tendo como objetivo básico o compartilhamento de recursos uns com outros. As redes estão ao nosso redor, até mesmo dentro de nós.

Nosso próprio organismo é uma rede interligada de órgãos. Na atual sociedade, as redes estão presentes na comunicação (TV/Rádio, celular, Internet, telefone, compra com cartão de crédito/débito), nas necessidades básicas (rede de esgoto, rede de energia elétrica, rede de abastecimento de água) e na nossa vida social (relacionamentos, amizades, família). Enfim, estamos e fazemos parte de várias redes.

Desde os primórdios a comunicação é uma das maiores necessidades da sociedade humana. Portanto tornou-se um desafio aproximar as comunidades mais distantes e facilitar a comunicação entre elas. Com a união dos computadores e das comunicações os sistemas computacionais sofreram uma profunda mudança na sua organização.

Como dito inicialmente, as redes de computadores surgiram da necessidade de se compartilhar recursos especializados para uma maior comunidade de usuários geograficamente dispersos.

Histórico

As redes de computadores foram criadas inicialmente para suprir uma necessidade militar. A década dos anos 60 foi um período de grande tensão entre as duas maiores potencias dessa época, isto é, os Estados Unidos da América e a União Soviética. Os americanos iniciaram programas de pesquisas para encontrar uma forma de interconectar os vários centros de comando do país, de modo que o seu sistema de informações seja robusto, ou seja, que continuasse funcionando mesmo que houvesse um conflito nuclear. Com o fim da guerra fria, esta estrutura passou a ser utilizada para uso científico e educacional.

No Brasil, as universidades foram as primeiras a se beneficiarem com essa estrutura de rede. Os serviços disponíveis restringiam-se a correio eletrônico e transferência de arquivos. Somente em 1990, a Fapesp (Fundação de Amparo à Pesquisa de São Paulo) conectou-se com a Internet. A partir de abril de 1995, o Ministério das Comunicações e o Ministério da Ciência e Tecnologia decidiram lançar um esforço comum de implantação de uma rede integrada entre instituições acadêmicas e comerciais. Desde então vários fornecedores de acesso e serviços privados começaram a operar no Brasil.

A seguir estão algumas datas importantes na evolução das redes de computadores e dos protocolos:

- **1968** - Foi desenvolvido pela ARPA (Advanced Research Projects Agency) o primeiro **backbone**. O objetivo desse projeto era interligar as universidades e também a área militar.

- **1975** - A DARPA (Defence Advanced Research Projects Agency) que deu lugar a ARPA começou a desenvolver os protocolos TCP/IP.

- **1979** – Foi formado um comitê para comandar o desenvolvimento desses protocolos. Esse comitê se chamava ICCB - Internet Control and Configuration Board.

- **1983** - A DARPA concedeu os direitos do código dos protocolos TCP/IP à Universidade da Califórnia para que fosse distribuído em sua versão UNIX. A DARPA pediu a todos os computadores que estavam conectados a ARPANET para que

usassem os protocolos TCP/IP. Esses protocolos se difundiram rapidamente, em razão de não ser um aplicativo comercial.

- **1985** - A Fundação Nacional de Ciência dos Estados Unidos (NSF) criou a NSFNET, que era uma rede de alta capacidade destinada a atender, tanto nos EUA como em outros paises, as entidades científicas e de pesquisa.
- **1989** - A ARPANET deu lugar a NSFNET, bem como o ICCB foi substituído pela Internet Advisory Board (IAB). A IAB possuía dois grupos principais: o IRTF (Internet Research Task Force) e o IETF (Internet Engeneering Task Force).
- **1995** - Muitas redes foram criadas ou desenvolvidas objetivando a melhora do tráfego de informações via Internet. Deu-se ainda nessa década a conexão de muitos setores à Internet, visando prestar e obter serviços pela rede.

Evolução dos Sistemas de Computação

Na década de 50, computadores eram máquinas grandes e complexas, operadas por pessoas altamente especializadas. Usuários enfileiravam-se para submeter suas leitoras de cartões ou fitas magnéticas que eram processados em lote. Não havia nenhuma forma de interação direta entre usuários e máquina.

Graças ao avanço na década de 60, foram desenvolvidos os primeiros terminais interativos, que permitiam aos usuários acesso ao computador central através de linhas de comunicação. Foi criado um mecanismo que viabilizava a interação direta com o computador, e outros avanços nas técnicas de processamento deram origem aos sistemas de tempo compartilhado (time-sharing), permitindo que várias tarefas dos diferentes usuários ocupassem simultaneamente o computador central, revezando o tempo de execução do processador.

Na década seguinte, foram feitas mudanças nos sistemas de computação, onde um sistema único centralizado transformou-se em um de grande porte, que estava disponível para todos

os usuários de uma determinada organização. Com o desenvolvimento dos microcomputadores, tornou-se viável a instalação em locais distintos, pois não era mais necessário concentrar esses equipamentos em determinada área específica.

Tornava-se então cada vez mais necessário que os dados ficassem armazenados em sistemas de grande porte e centralizados e compartilhados e os periféricos interconectados. Foi possível então trabalhar em ambientes de trabalho cooperativos interligando recursos não só no âmbito industrial como no acadêmico.

Problemas de desempenho surgiram, mas em resposta foram criadas novas arquiteturas que possibilitavam a distribuição e o paralelismo melhorando o desempenho, a confiabilidade e modularidade dos sistemas computacionais.

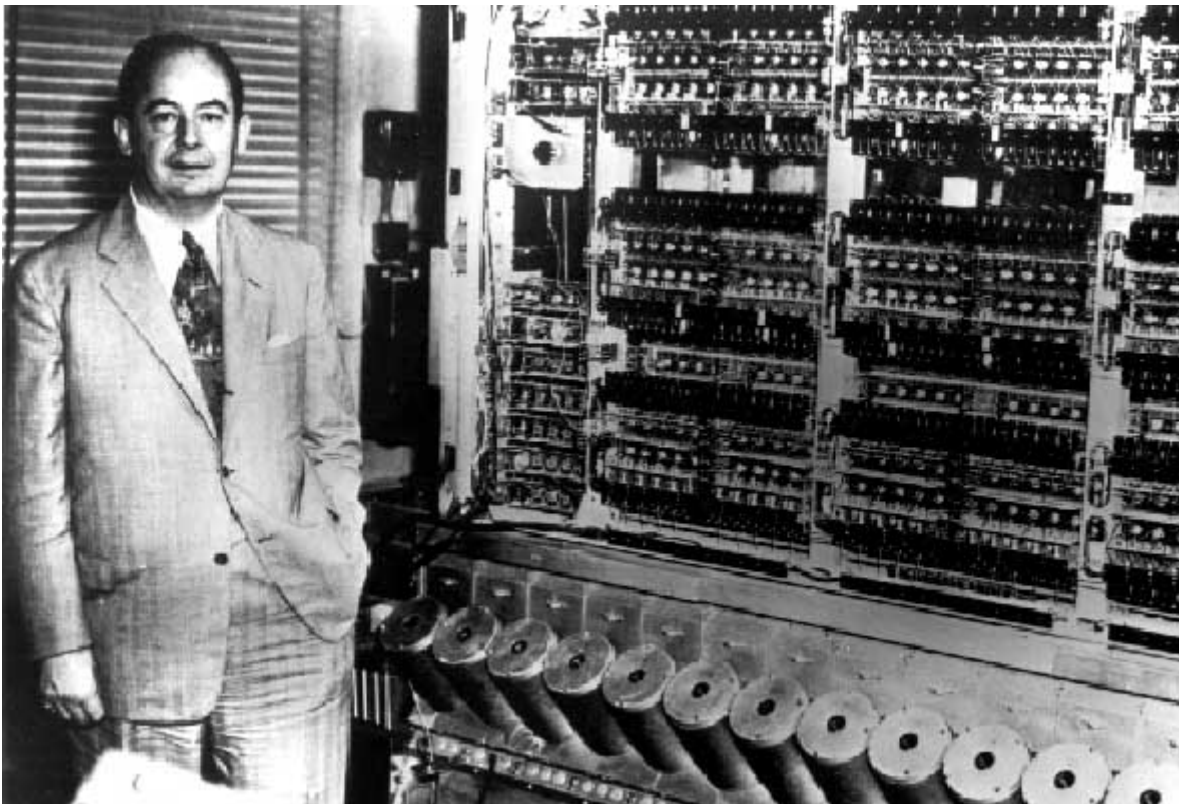
Evolução das Arquiteturas de Computação

A maioria dos computadores projetados até a década de 80 teve sua concepção baseada nos modelos originais do matemático húngaro-americano John Louis Von Neumann.

Von Neumann foi um personagem crucial no desenvolvimento científico e tecnológico da segunda metade do século XX. Contribuiu decisivamente para mudar a história da Inteligência Artificial e criou a conhecida "arquitetura de Von Neumann" para computadores com unidade de armazenamento e memória tornando viável o modelo básico criado por Alan Mathison Turing. Em 1951, o primeiro computador eletrônico, o EDVAC (Electronic Discrete Variable Automatic Computer), foi concluído, seguindo a proposta de Von Neumann.

Von Neumann propôs que as instruções fossem armazenadas na memória do computador, pois elas eram lidas de cartões perfurados e executadas na hora, uma a uma. Armazenando-as na memória para depois executá-las, tornaria o computador mais rápido, já que, no momento da execução, as instruções seriam obtidas com rapidez eletrônica.

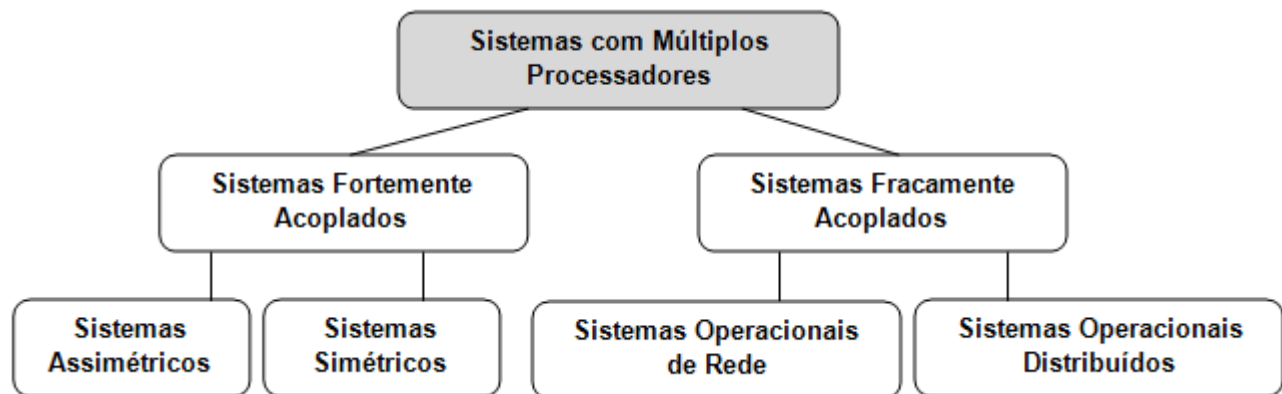
A maioria dos computadores atuais ainda segue o modelo proposto pelo matemático, onde um computador sequencial digital que processa informações passo a passo, ou seja, os

mesmos dados de entrada produzem sempre a mesma resposta. A interação perfeita entre o modo como os programas são desenvolvidos e a maneira como são interpretados foi uma das razões para o grande sucesso desse modelo.

1951 - John Louis Von Neumann ao lado do EDVAC

Sistemas Fortemente Acoplados e Fracamente Acoplados

A revolução nos sistemas de computadores começou com os avanços da tecnologia dos circuitos integrados (chips), que reduziram em muito os custos. Várias arquiteturas foram então propostas, tentando contornar as limitações de confiabilidade, custo e desempenho.

Surgiu então a ideia de sequências múltiplas e independentes de instruções em um sistema composto por vários elementos de processamento, conhecido como Sistemas Fortemente

Acoplados onde dois ou mais processadores compartilham uma única memória e são controlados por apenas um único sistema operacional. Tais sistemas são geralmente utilizados no processamento de aplicações que fazem uso intensivo da CPU, onde o processamento é voltado para a solução de um único problema.

Depois surgiram os sistemas fracamente acoplados que possuíam dois ou mais sistemas de computação, conectados através de linhas de comunicação. Cada sistema funcionava de forma independente, possuindo seu(s) próprio(s) processador(es), memória e dispositivos. A utilização de sistemas fracamente acoplados caracteriza-se pelo processamento distribuído entre os seus diversos processadores. A diferença principal entre os dois sistemas está no espaço de endereçamento (memória) compartilhado por todos os processadores nos sistema fortemente acoplado, enquanto nos sistemas fracamente acoplados cada sistema tem sua própria memória individual. Além disso, a taxa de transferência entre CPUs e memória em sistemas fortemente acoplados é normalmente maior que nos fracamente acoplados.

Abaixo seguem várias razões para o uso de sistemas de múltiplos processadores (fortemente ou fracamente acoplados):

- **Custo/desempenho**: A evolução da tecnologia de síntese de circuitos integrados tem conduzido os custos de microprocessadores e memórias a valores bem reduzidos;

- **Versatilidade**: Um sistema de múltiplos processadores pode apresentar um grande potencial de processamento, podendo ser moldado à aplicação;
- **Modularidade**: O fato de um sistema de computação modular aumenta a relação custo/desempenho, pois poderá ser utilizado para diversas configurações, acompanhando o crescimento e facilitando a manutenção do mesmo;
- **Concorrência**: Máquinas destinadas a aplicações que necessitam alto desempenho requerem a utilização de processamento concorrente.

Algumas desvantagens de um sistema de múltiplos processadores de acordo com os requisitos particulares do sistema:

- O desenvolvimento de aplicativos para tais sistemas pode ser mais complexo e muito complicado, o que aumenta o custo;
- A decomposição das tarefas é mais complexa mesmo que realizada pelo software;
- O desenvolvimento do software de diagnóstico é muito complexo;
- Uma falha na estrutura de comunicação pode comprometer outros processos.

Sistemas Assimétricos e Simétricos

Inicialmente, os sistemas com múltiplos processadores estavam limitados aos sistemas de grande porte, restritos ao ambiente universitário e às grandes corporações. Com a evolução dos computadores pessoais e estações de trabalho os sistemas multitarefa evoluíram para permitir a existência de vários processadores no modelo assimétrico e simétrico.

No multiprocessamento assimétrico somente um processador principal executa serviços do sistema operacional. Sempre que um processador secundário precisar realizar outra operação, terá de requisitar o serviço ao processador principal. Dependendo do volume de

tarefas destinadas aos processadores secundários, o sistema pode se tornar indisponível, em razão do elevado número de interrupções que são feitas pelo processador principal.

Em outra situação se o processador principal falhar, o sistema para, necessitando ser configurado para que o processador secundário assuma a função de principal. Mas este tipo de sistema não utiliza de forma satisfatória o hardware, em razão da assimetria dos processadores, que não realizam as mesmas funções.

Em um sistema simétrico (já o nome o indica) os processadores trabalham de forma simétrica, ou seja, todos os processadores podem realizar as mesmas funções independentemente, praticamente todos têm a mesma hierarquia, a não ser a inicialização do sistema que é executada pelo processador principal. Qualquer programa poderá ser executado por qualquer processador ou por mais de um ao mesmo tempo de forma paralela.

Quando existe falha em um dos processadores, mesmo sendo o principal, o sistema continua em funcionamento sem a necessidade de interferência manual, porém o sistema operará com menor capacidade de processamento.

O uso de mais de um processador faz com que o acesso à memória possa ser simultâneo, podendo causar algum conflito. Ficando a cargo do hardware e do sistema operacional gerenciar esses acessos e (se possível) solucionar os possíveis conflitos que possam ser criados por eles.

Os sistemas simétricos são mais eficientes que os assimétricos, pois possibilitam melhor gerenciamento do processamento e das operações de entrada/saída, apesar de ser a sua implementação bastante complexa.

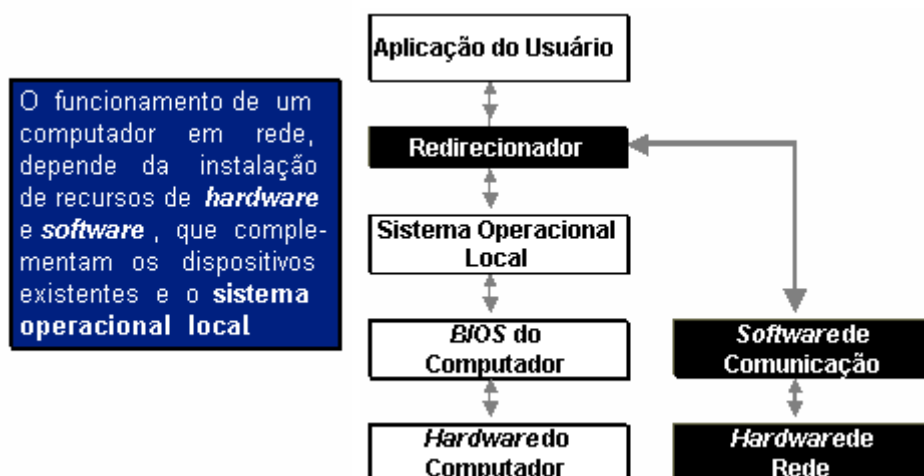
UNIDADE 2

Objetivo: Saber qual a funcionalidade de um sistema operacional de rede.

Sistemas Operacionais de Rede

O Que é um Sistema Operacional de Rede

Basicamente, um sistema operacional de rede é um conjunto de módulos que ampliam as tarefas dos sistemas operacionais locais, complementando-os com um conjunto de funções básicas, e de uso geral, que tornam transparente o uso de recursos compartilhados da rede.

Portanto, um computador de rede tem o sistema operacional local interagindo com o sistema operacional de rede, para que possam ser utilizados os recursos de rede tão facilmente quanto os recursos na máquina local. Em efeito, o sistema operacional de rede coloca um redirecionador entre o aplicativo do cliente e o sistema operacional local para redirecionar as solicitações de recursos da rede para o programa de comunicação que vai buscar os recursos na própria rede.

O sistema operacional de rede, portanto, controla os sistemas e dispositivos dos computadores em uma rede e permite que se comuniquem uns com os outros. Normalmente o modelo de operação do sistema operacional de rede é o modelo Cliente/ Servidor, ou seja, o ambiente onde o processamento da aplicação é compartilhado com outro cliente (que solicita um serviço) e um ou mais servidores (prestam esses serviços). Os tipos de arquiteturas para sistemas operacionais de rede podem ser:

- **Peer-to-Peer**: Nestas redes todos poderiam ser (ou não) servidores, mas certamente todos são clientes, normalmente neste tipo de redes os servidores são não dedicados, mas nada impediria o contrario.
- **Cliente/Servidor**: Nestas redes podem existir dois tipos:
    - Servidor Dedicado
    - Servidor não Dedicado

No caso dos sistemas Cliente/Servidor o sistema cliente possui características mais simples, voltadas para a utilização de serviços, enquanto que o sistema do servidor possui maior quantidade de recursos, com o único propósito de serem disponibilizados aos clientes da rede. Os sistemas baseados em Unix são potencialmente clientes e servidores, sendo feita a escolha durante a instalação dos pacotes, enquanto que os sistemas Windows, existem versões clientes (Windows 2000 Professional, Windows XP) e versões servidores (Windows 2000 Server, Windows 2003 R2 e Windows 2008 Server). A seguir os principais sistemas operacionais de rede.

Sistemas UNIX

O sistema UNIX foi criado nos Laboratórios Bell em 1970 por Ken Thompson, Dennis Ritchie e Brian Kernigham, entre outros, para ajudar no controle dos projetos internos do próprio laboratório. Era um sistema básico e voltado principalmente para programadores e cientistas.

Durante o ano de 1975, Ken Thompson quando trabalhava como professor assistente na Universidade da Califórnia, em Berkeley, continuou a desenvolver o sistema UNIX projetado inicialmente nos laboratórios da Bell (Bell Lab). Este desenvolvimento foi tomado pelos outros professores e alunos, que desenvolveram uma série de melhorias no sistema original. Estas melhorias geraram um sistema operacional com algumas diferenças em relação ao sistema UNIX do Bell Lab. e passou a ser conhecido como o "UNIX de Berkeley". Algumas empresas começaram a comercializar esta versão do sistema operacional, sendo a mais conhecida a versão chamada SunOS da Sun Microsystems.

1972 - Ken Thompson e Dennis M. Ritchie com o PDP-11

Em 1979, a AT&T resolveu lançar comercialmente o UNIX. Esta versão ficou sendo conhecida como "Versão 7". Após algum tempo, em 1982, alguns problemas da versão 7

foram corrigidos e foi lançada a versão chamada de "System III" (Sistema Três). A partir deste ponto, houve uma evolução paralela de dois "tipos" de UNIX. Uma comercializada pela AT&T e outra proveniente da Universidade da Califórnia.

Até 1983, o uso do UNIX estava principalmente voltado para aplicações científicas, sendo o sistema mais utilizado no meio acadêmico. Neste ano, a AT&T resolveu agregar uma série de características e facilidades, visando assim, o usuário comercial. Este procedimento sempre encontrou barreiras, pois o usuário comercial achava que o UNIX era por demais científico e nada user friendly (amigável), sendo só usado por programadores e cientistas. A versão comercial ficou sendo conhecida como "System V" (Sistema Cinco).

A partir de 1989 foram formados pelas maiores empresas na área de computação dois grandes consórcios, visando uma unificação e padronização de todos os sistemas UNIX existentes no mercado. Esta padronização é necessária para que se tenha uma portabilidade de todas as aplicações desenvolvidas para UNIX, dando assim uma força maior de penetração do UNIX no mercado comercial. Ao contrário do que aconteceu no Brasil, onde o UNIX foi um substituto para minicomputadores e movia basicamente sistemas multiusuários com terminais burros, no exterior o UNIX era o sistema High-end, de alto desempenho, em redes e gráfico, só encontrando alguma concorrência no NT.

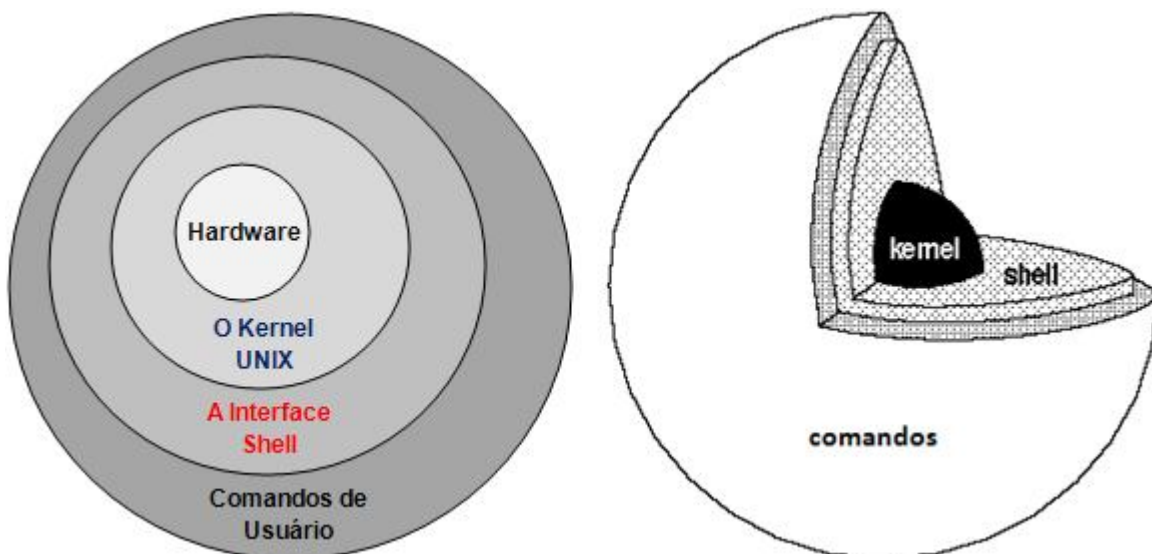
O UNIX E A Internet

Os Laboratórios Bell usavam computadores com diferentes arquiteturas (o que dificultava muito a comunicação entre os diferentes usuários das diferentes arquiteturas), o sistema operacional UNIX teve em conta certa portabilidade. O principal objetivo deste novo sistema era que pudesse ser instalado e utilizado em diferentes plataformas de computação.

Um grupo de pesquisadores da Universidade da Califórnia, em Berkeley, interessou-se particularmente pelo UNIX e desenvolveu para ele um conjunto de aplicações, chegando mesmo a modificar o Kernel (núcleo) do sistema operacional. Estas modificações levaram à implementação de novas funcionalidades em particular com as comunicações para o

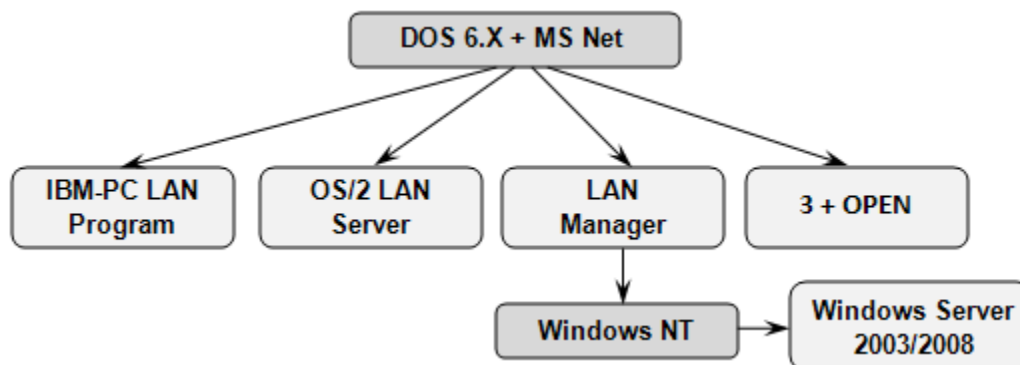
trabalho entre redes (em inglês Inter – Networks), termo que logo seria conhecido simplesmente como Internet.

A versão UNIX de Berkeley - SD UNIX (Berkeley Software Distribution) foi também disponibilizada às universidades norte-americanas, que licenciaram o código do UNIX do Bell Labs e fomentaram o desenvolvimento de versões paralelas do UNIX. A maior delas foi o BSD UNIX, da Universidade da Califórnia em Berkeley. Ele foi a base do desenvolvimento da ARPANET e seu famoso conjunto de protocolos conhecido como TCP/IP. Desta forma surgiu a Internet, iniciada essencialmente com caráter militar e científico/acadêmico até a explosão comercial da atualidade e quase que inteiramente desenvolvida e implementada pelo sistema operacional UNIX.

Atualmente, o UNIX System V é o padrão internacional de fato no mercado UNIX, constando das licitações de compra de equipamentos de grandes clientes na América, Europa e Ásia.

Atualmente, UNIX é o nome dado a uma grande família de Sistemas Operativos que partilham de muitos dos conceitos dos Sistemas Unix originais, sendo todos eles desenvolvidos em torno de padrões como o POSIX (Portable Operating System Interface) e outros. Alguns dos Sistemas Operativos derivados do UNIX são: BSD (FreeBSD, XFree86,

OpenBSD e NetBSD), Solaris (anteriormente conhecido por SunOS), IRIX, AIX, HP-UX, Ultrix, Tru64, Linux (nas suas centenas de distribuições), e até o MacOS X (baseado em um Kernel Mach BSD chamado Darwin). Existem mais de quarenta sistemas operacionais do tipo UNIX, rodando desde celulares a supercomputadores, de relógios de pulso a sistemas de grande porte.

A Família Microsoft

A figura abaixo apresenta os sistemas operacionais que antecederam à família Windows NT e Windows Server 2003/2008:

Soluções Microsoft

- Família Windows XP: Home, Professional (32 bits) e a versão para 64 bits.
- Família Windows 2000: Professional, Server, Advanced Server, Datacenter Server.
- Windows CE e Embedded
- Windows Vista
- Família Windows .NET Server 2003: Web Server, Standard Server, Enterprise Server e Datacenter Server

- Windows Server 2008

A Família Windows XP

Oriundo do Windows 2000 e do Windows Millennium possue o Kernel (núcleo) do Windows 2000. Foram lançadas três versões: Home (antigo ME), Professional (que é o antigo 2000 Professional) com suporte para uma arquitetura de 64 bits. A versão para 64 bits tem capacidade de endereçar 64 GBytes de RAM e está otimizada para a família de processadores Intel Itanium. Também possui suporte de multiprocessamento para dois processadores Intel Itanium.

A Família Windows 2000 Server

Aqui temos as seguintes versões:

- Server – 1 a 4 processadores e 4 GB de RAM, arquitetura de 32 Bits;
- Advanced Server – 1 a 8 processadores e 8 GB de RAM, arquitetura de 64 Bits;
- Datacenter Server – 1 a 32 processadores e 64 GB de RAM, arquitetura de 64 Bits.

A Família Windows .NET Server 2003 R2

Próxima versão do Windows 2000 Server;

Várias versões: Web, Standard, Enterprise, Datacenter.

Segue abaixo uma tabela com alguns recursos do Windows.NET Server 2003.

Chave: ● = Recurso incluído ◒ = Recurso com suporte parcial ○ = Recurso não incluído

Recurso	**Servidores Web**	**Standard Server**	**Enterprise Server**	**Datacenter Server**
Tecnologias de Cluster				
Balanceamento de carga da rede	●	●	●	●
Cluster de falhas	○	○	●	●
Comunicações e Serviços de Rede				
Conexões de rede virtual privada (VPN)	◒	●	●	●
Serviço de protocolo de início de sessão (SIP)	○	●	●	●
Serviço de autenticação da Internet (IAS)	○	●	●	●
Ponte de rede	○	●	●	○

Compartilhamento de conexão com a Internet (ICS)	○	●	●	○
Serviços de Diretório				
Active Directory™	○	●	●	●
Suporte para serviços de metadiretório (MMS)	○	○	●	●
Serviços de Arquivo e Impressão				
Sistema de arquivos distribuídos (DFS)	●	●	●	●
Sistema de arquivos com criptografia (EFS)	●	●	●	●
Restauração de cópia duplicada	○	●	●	●
SharePoint™ Team Services	○	●	●	●
Armazenamento removível e remoto	○	●	●	●

Serviço de fax	○	●	●	●
Serviços para Macintosh	○	○	●	●
Serviços de Gerenciamento				
IntelliMirror	○	●	●	●
Conjunto de diretivas resultante (RSoP)	○	●	●	●
Windows Management Instrumentation (WMI)	○	●	●	●
Servidor de instalação remota (RIS)	○	●	●	●
Serviços de Segurança				
Firewall de conexão com a Internet	○	●	●	○
Serviços de certificado	○	◒	●	●

Serviços de Terminal				
Área de trabalho remota para administração	●	●	●	●
Terminal Server	○	●	●	●
Diretório de sessão do Terminal Server	○	○	●	●
Serviços de Multimídia				
Windows Media™ Services	○	●	●	○
Escalonabilidade				
Suporte a 64 bits para computadores Intel® Itanium™	○	○	●	●
Memória com adição a quente[1]	○	○	●	●
Acesso não uniforme à memória (NUMA) [1]	○	○	●	●

Controle de processos	○	○	●	●
Programa de suporte a Datacenter	○	○	○	●
Serviços de Aplicativos de Web				
.NET Framework	●	●	●	●
Internet Information Services (IIS)	●	●	●	●
ASP.NET	●	●	●	●

[1] Pode ser limitado devido à falta de suporte pelo hardware OEM.

O Windows Server 2003 R2 amplia o sistema operacional Windows Server 2003, fornecendo uma forma mais eficaz de gerenciamento e controle de acesso a recursos locais e remotos enquanto se integra facilmente ao ambiente existente do Windows Server 2003. O Windows Server 2003 R2 fornece uma plataforma Web escalonável e segurança melhorada, interoperabilidade contínua com sistemas UNIX e permissão de novos cenários, incluindo o gerenciamento remoto simplificado do servidor, melhoria de identidade e gerenciamento de acessos, além de um gerenciamento mais eficaz de armazenamento.

O Windows Server 2003 R2 Enterprise Edition também distribui novas licenças dinâmicas que permitem aos clientes um valor maior através da virtualização de seu servidor. Esta página fornece uma visão geral dos benefícios, novos recursos e melhorias no Windows Server 2003 R2. Com base na segurança melhorada, na confiabilidade e no desempenho fornecidos pelo Windows Server 2003 Service Pack 1 (SP1), o Windows Server 2003 R2

amplia a conectividade e o controle a recursos locais e remotos. As empresas podem se beneficiar de seus custos reduzidos e eficácia maior, conseguida através do gerenciamento otimizado e controle sobre os recursos da empresa.

O Windows Server 2003 R2 permite a manutenção do desempenho, disponibilidade e benefícios de produtividade de um servidor em um escritório filial ao evitar problemas tipicamente associados com soluções de servidores como limitação de conectividade e despesas de gerenciamento.

O Windows Vista

O lançamento da versão da Microsoft Windows Vista ocorre a mais de cinco anos após o lançamento do Windows XP (a versão anterior do sistema operacional desktop da Microsoft) fazendo deste período o mais longo entre lançamentos consecutivos de versões do Windows. Oficialmente o Windows Vista foi disponibilizado ao público em Novembro de 2007.

O Windows Vista possui centenas de novos recursos e funções, como uma nova interface gráfica do usuário, funções de busca aprimoradas, novas ferramentas de criação multimídia como o Windows DVD Maker, e completamente renovadas aplicações para redes de comunicação, áudio, impressão e subsistema de exibição. O Windows Vista também tem como alvo aumentar o nível de comunicação entre máquinas em uma rede doméstica usando a tecnologia Peer-to-Peer, facilitando o compartilhamento de arquivos e mídia digital entre computadores e dispositivos.

Para aqueles que o desenvolveram, o Vista introduz a versão 3.0 do Microsoft.NET Framework, que tem como alvo tornar significativamente mais fácil o caminho para os que buscam desenvolver aplicativos de alta qualidade com a tradicional Windows API.

Uma das mais comuns críticas ao Windows XP e aos seus predecessores são as suas geralmente exploradas vulnerabilidades de segurança e a total susceptibilidade a malware, vírus e buffer overflows. Em consideração a isso, o então presidente da Microsoft, Bill Gates,

anunciou no começo de 2002 uma iniciativa de Computação Confiável de grande escala na empresa que tinha como objetivo desenvolver a segurança nos softwares desenvolvidos pela empresa.

Segundo a Microsoft, esta versão do Windows vem com uma tecnologia de bloqueio que evita o funcionamento de cópias não autorizadas. Esta tecnologia limita o uso da plataforma restringindo as suas funcionalidades caso o usuário não ative o sistema em um prazo de 30 dias, mas já existem cracks disponíveis na Internet que conseguem quebrá-lo. Existia no Windows XP um sistema parecido, denominado WPA (Windows Product Activation), que avisa quando o usuário estava usando uma cópia não autorizada do sistema, mas que também já foi inteiramente quebrado por crackers.

De acordo com a Microsoft, computadores que podem executar Windows Vista são classificados com "Vista Capable" e "Vista Premium Ready". Um Vista Capable ou PC equivalente precisa ter no mínimo um processador de 800 MHz, 512 MB de RAM e uma placa gráfica de classe DirectX 9, e não será capaz de suportar os gráficos "high end" do Vista, incluindo a interface do usuário Aero.

Um computador Vista Premium Ready terá a vantagem da função "high end" do Vista, mas precisará no mínimo de um processador de 1 GHz, 1 GB de memória RAM, e uma placa gráfica Aero-compatível com no mínimo 128 de memória gráfica e suportando o novo Windows Display Driver Model. A companhia também oferece uma beta do Windows Vista Upgrade Advisor através do seu site Web para determinar a capacidade de um PC para executar o Vista em seus vários modos.

O utilitário é somente executável no Windows XP. Mas percebe-se que a maioria dos PCs atuais atende às necessidades do novo Windows. Atualmente, chama-se Designed For Windows Vista (Versão).

Os requisitos de Hardware para a instalação do Windows Vista são listados na tabela abaixo:

Hardware	Mínimo	Recomendado
Processador	800 MHz	2 GHz (Dual Core)
Memória RAM	512 MB	2 GB
GPU (Graphic Processor Unit)	DirectX 9 capaz	GPU capaz DirectX 9 com Hardware Pixel Shader v2.0 e suporte Driver WDDM.
Memória do GPU	64 MB RAM	128MB de RAM ou 256MB para maior resolução de vídeo.
Capacidade do HD	20 GB	80 GB
Espaço livre do HD	15 GB	20 GB
Tipo de HD	Normal	Normal com memória flash/disco rígido Híbrido.
Outros drivers	CD-ROM	DVD-ROM

O Windows Server 2008

O Windows Server 2008 é o mais recente lançamento da linha de sistemas operacionais para servidores Windows. É o sucessor do Windows Server 2003, que fora lançado há (quase) cinco anos. Assim como o Windows Vista, o Windows Server 2008 foi projetado sobre o Kernel (núcleo) do Windows NT 6.0.

O Windows Server 2008 foi lançado oficialmente em Março de 2008 e apresenta, aos usuários, várias melhoras em relação às versões anteriores, entre elas podemos mencionar as seguintes:

- **Novo processo de reparação de sistemas NTFS**: o processo em segundo plano que repara os arquivos danificados.

- **Criação de sessões de usuário em paralelo**: redução dos tempos de espera nos Terminal Services e na criação de sessões de usuário de grande escala.
- **Fechamento limpo de Serviços**: os tempos longos de espera antes da finalização de serviços são praticamente eliminados.
- **Kernel Transaction Manager**: melhoras na gestão concorrente de recursos.
- **Sistema de arquivos SMB2**: o acesso aos servidores multimídia torna-se de 30 a 40 vezes mais rápido.
- **Address Space Load Randomization (ASLR)**: proteção contra malware durante o carregamento de drivers na memória.
- **Windows Hardware Error Architecture (WHEA)**: protocolo melhorado e padronizado para reporte de erros.
- **Virtualización de Windows Server**: melhoras no desempenho da virtualização.
- **PowerShell**: inclusão de uma console melhorada com suporte gráfico (GUI) para administração do sistema.
- **Server Core**: o núcleo do sistema renovou-se com muitas e novas características. Porem o Server Core não possui uma interface gráfica (GUI) para as configurações. A maioria destas características deve ser configurada via linha de comando ou remotamente. Entre as principais características do Server Core temos: Ativação do Produto, Configuração de Vídeo, Configuração de Horário e Time Zone, Remote Desktop, Gerenciamento de Usuários locais, Firewall, WinRM (remote shell), Configurações de IP, Nome do Computador/ Domínio, Instalação de Features e Roles.

A Família Netware

Sistema operacional de rede da Novell que ainda é muito utilizado no mundo todo. É o primeiro sistema operacional de rede para um compartilhamento real de arquivos. Foi o

primeiro sistema operacional de rede para PCs baseado no sistema operacional DOS. Desenvolvido pela Novell, o NetWare é um sistema proprietário usando multitarefa cooperativa para executar muitos serviços em um computador, e os protocolos de rede são baseados no arquétipo da Xerox XNS. Atualmente suporta TCP/IP junto com o próprio IPX/SPX.

A origem do sistema operacional Netware se remonta no inicio da década dos 80. Foi criado em 1982, em Provo (Utah) pela empresa SuperSet (atual Novell) e foi líder de mercado (80%) entre 1985 e 1995. Ainda possui maior desempenho do mercado como Servidor de Arquivo e foi o primeiro a oferecer proteção no Nível III (Espelhamento de Servidores).

DOS 3.X + NETWARE (NOVELL)

Os níveis mencionados a seguir são referentes aos níveis do modelo OSI que será explicado em detalhe mais adiante na Unidade 13. Nesse sentido, a família Netware utiliza:

- Para os níveis 3, 4 e 5 (de Rede, Transporte e Sessão): O padrão IPX/SPX (Novell);
- Para o nível 6 (de Aplicação): O padrão NVT (Network Virtual Terminal) e o NCP (Netware Core Protocol) ambos desenvolvidos pela Novell;

O Netware também é conhecido pelas suas características:

- Desempenho, confiabilidade e segurança;
- O servidor de rede Netware é um servidor dedicado.
- É uma rede que funciona com o modelo Cliente/Servidor.

Algumas características

- Verificação de leitura após escrita;
- HOT-FIX da Tabela de blocos inutilizáveis.
- TTS (Transaction Tracking System): Uma ferramenta de proteção a bases de dados.
- Bindery na versão 3.x e NFS na versão 4.x e 6.x.

A Família Linux

O sistema operacional Linux é um sistema baseado no UNIX. Foi desenvolvido por Linus Torvalds, inspirado no sistema Minix. O Linux é um dos mais proeminentes exemplos de desenvolvimento com código aberto e de software livre. O seu código fonte está disponível sob licença GPL (GNU Public License) para qualquer pessoa utilizar, estudar, modificar e distribuir de acordo com os termos da licença. Inicialmente desenvolvido e utilizado por grupos de entusiastas em computadores pessoais, o sistema Linux passou a ter a colaboração de grandes empresas, como a IBM, a Sun Microsystems, a Hewlett-Packard, e a Novell, ascendendo como um dos principais sistemas operacionais para servidores -- oito dos dez serviços de hospedagem mais confiáveis da Internet utilizam o sistema Linux nos seus servidores Web. Existem sistemas Linux para diversas arquiteturas computacionais, como supercomputadores, microcomputadores e aparelhos celulares.

O kernel Linux foi, originalmente, escrito (na linguagem C) por Linus Torvalds do Departamento de Ciência da Computação da Universidade de Helsinki, Finlândia, com a ajuda de vários programadores voluntários através da Usenet. O Linux é um sistema operacional com todas as características dos sistemas UNIX, mas para processadores com arquitetura Intel x86 e x/64 de 32 e 64 bits respectivamente. Existe um número grande de diferentes distribuições (distros), mas o núcleo (Kernel) do sistema Linux basicamente é o mesmo para cada uma delas. A seguir uma tabela com algumas (das várias) distribuições Linux:.

Quadro com algumas (das várias) distribuições Linux:

Nome	**Plataforma**
Redhat Linux	Intel, Alpha, Itanium.
SCO/Caldera Linux	Intel
Conectiva Linux	Intel (em portugues)
Linux-Mandrake	Intel, PowerPC
S.u.S.e. Linux	Intel, PowerPC, Alpha, Sparc, Itanium, Mainframes...
Debian GNU/Linux	PowerPC, Alpha, Sparc, ...
Turbo Linux	Intel,...
MkLinux (Apple)	Intel, PA-RISC, PowerPC
Slackware	Intel, Alpha, Sparc
Ubuntu	Intel (x86 e x64), Sparc

Os sistemas operacionais de rede não diferem daqueles usados em máquinas monousuário. Obviamente, eles precisam de uma interface controladora de rede e de um software específico para gerenciar tal interface, além de programas que permitam a ligação de usuários a máquinas remotas e seu acesso a arquivos também remotos. Tais características não chegam a alterar a estrutura básica do sistema operacional usado para máquinas com um único processador. Já os sistemas operacionais distribuídos precisam de mais do que uma simples adição de algumas linhas de código a um sistema usado em máquinas monoprocessadas, pois tais sistemas diferem dos centralizados em pontos muito críticos.

Por exemplo, os sistemas operacionais distribuídos permitem que programas rodem em vários processadores ao mesmo tempo, necessitando, portanto de algoritmos de

escalonamento de processador bem mais elaborados e complexos, de forma a otimizar o grau de paralelismo disponível no sistema.

O melhor exemplo da utilização dos sistemas operacionais de rede são as redes locais, conhecidas como redes LAN. Nesse ambiente, cada estação pode compartilhar seus recursos com o restante da rede. Caso um computador sofra qualquer problema, os demais componentes da rede poderiam continuar com o processamento, apenas não dispondo dos recursos oferecidos por este.

Sistemas Distribuídos

Assim como nos sistemas operacionais de rede, cada estação (de um sistema distribuído) também possui seu próprio sistema operacional, mas o que caracteriza como sendo um sistema distribuído (também conhecido como cluster) é a existência de um relacionamento mais forte entre os seus componentes (processadores), onde geralmente (mas não necessariamente) os sistemas operacionais são os mesmos, funcionando como um único sistema centralizado. Um sistema Distribuído é formado por um conjunto de módulos processadores interligados por um sistema de comunicação (cabos de rede ou canais de transmissão de dados).

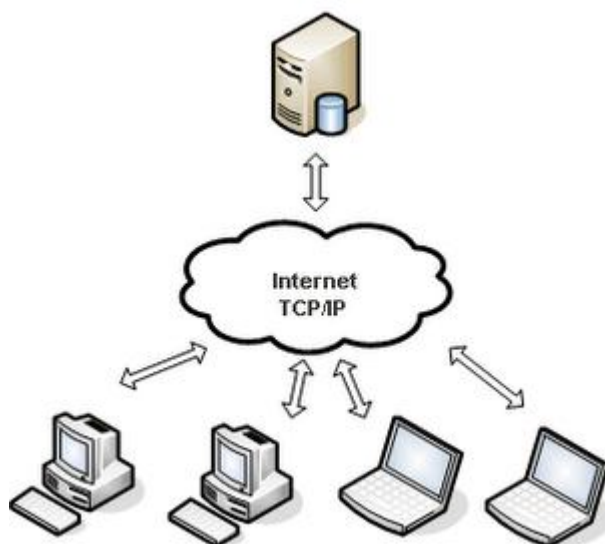
Como as aplicações são distribuídas, a redundância é uma grande vantagem, pois quando há problema com um dos componentes (processador) outro assume a tarefa em questão.

Alguns fabricantes, juntamente com órgãos de padronização, definiram padrões para a implementação de sistemas distribuídos. O Distributed Computing Enviroment (DCE), o Common Object Request Broker Architecture (CORBA) e o Object Linking and Embedding (OLE) são alguns dos padrões para o desenvolvimento de aplicações em ambientes distribuídos.

Um sistema de computo com arquitetura distribuída pode possuir um número ilimitado de módulos autônomos para processamento, interconectados de tal forma que, para o usuário final, o sistema todo se apresente como uma única máquina, no qual o controle geral é implementado através da cooperação de elementos descentralizados. Uma rede de computadores também pode (em teoria) estar formada por um número ilimitado de estações, mas a independência dos vários módulos de processamento é preservada em razão da tarefa de compartilhamento de recursos e troca de informações, em outras palavras, em uma rede de computadores a troca de informações entre os diferentes computadores não é tão elevada se comparada com um sistema de computo com arquitetura distribuída onde a comunicação entre os diferentes processadores é crítica e extremamente elevada.

Lembrar que o objetivo de um sistema distribuído é comum para todos os módulos de processamento, todos eles devem desenvolver tarefas intimamente relacionadas para um determinado objetivo, daí que a comunicação entre todos os processadores do sistema deve ser elevada e muito bem coordenada.

Um exemplo prático (e muito interessante) de um sistema distribuído é o projeto SETI (Search for Extra Terrestrial Intelligence). O projeto SETI, desenvolvido pela Universidade de Berkeley na Califórnia, é um experimento científico que utiliza o tempo ocioso dos computadores conectados à Internet para seu objetivo principal de procura por vida inteligente extraterrestre. Qualquer pessoa conectada à Internet pode participar basta rodar o programa gratuito disponível no site BOINC (http://boinc.berkeley.edu).

Basicamente, este programa permite que sua máquina disponibilize o tempo ocioso dela para fazer parte de projetos científicos, o projeto esta constituído por diferentes protetores de tela e é disponibilizado para as plataformas Windows, MacOS, e Linux.

O funcionamento básico sobre como a sua máquina chega a fazer parte do sistema distribuído desse projeto é o seguinte: Logo após da instalação do software, você deve configurar a sua máquina e escolher o protetor de tela do projeto em questão. Desta forma cada vez que a sua máquina ative o protetor de tela, devido a que você parou de utilizar ela (mas sem desligá-la e com conexão a Internet), a sua máquina fará parte de algum dos seguintes projetos: SETI@home, Climateprediction.net, Rosetta@home, World Community Grid, entre vários outros. Portanto, cada vez que o protetor de tela seja ativado a sua máquina fará parte, de forma automaticamente, do sistema distribuído de computo do projeto SETI, assim que você retome o uso da sua máquina, o protetor de tela será desativado e a máquina é liberada do sistema de computação distribuída do projeto SETI até a seguinte vez que o protetor de tela seja ativado novamente.

O pessoal encarregado de escrever e desenvolver esse projeto através de simples protetores de tela foi muito experto já que eles visavam praticamente todo o poder computacional de cada uma das máquinas que iriam fazer parte do projeto e eles só poderiam conseguir isso quando a máquina estiver ligada, conectada a Internet e praticamente parada, (teoricamente) só rodando o protetor de tela que é o software que permite que uma máquina seja parte do sistema distribuído, portanto, toda a capacidade de processamento da CPU estaria dedicada exclusivamente aos dados e cálculos enviados desde os processadores centrais do projeto para a sua máquina.

Inclusão Digital

Novas tecnologias e o acesso à Internet transformaram a sociedade brasileira e mundial na sociedade da informação. Mas grande parte da população ainda não tem acesso a esses recursos devido a vários fatores, como custos altos para a infraestrutura e ausência de interesses políticos para tanto.

Muitos órgãos mundiais vêm discutindo sobre esse assunto e principal documento que reconhece a importância da inclusão digital foi publicado pela

Organização das Nações Unidas (ONU) no final de 2003. Projetos coordenados em conjunto por empresas privadas, governo e a sociedade civil, são o ponto de partida para que se criem condições de acesso para as regiões e pessoas mais carentes.

Nesse sentido, a inclusão digital ou infoinclusão é a democratização do acesso às tecnologias da Informação, de forma a permitir a inserção de todos na sociedade da informação. Inclusão digital é também simplificar a sua rotina diária, maximizar o tempo e as suas potencialidades. Um indivíduo incluso digitalmente não é aquele que apenas utiliza essa nova linguagem, que é o mundo digital, para trocar e-mails, mas o que usufrui desse suporte para melhorar as suas condições de vida.

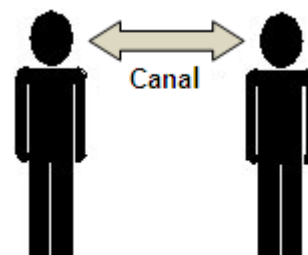
Entre as estratégias inclusivas estão projetos e ações que facilitam o acesso de pessoas de baixa renda às Tecnologias da Informação e Comunicação (TIC). A inclusão digital volta-se também para o desenvolvimento de tecnologias que ampliem a acessibilidade para usuários com deficiência.

Dessa forma, toda a sociedade pode ter acesso a informações disponíveis na Internet, e assim produzir e disseminar conhecimento. A inclusão digital insere-se no movimento maior de inclusão social, um dos grandes objetivos compartilhados por diversos governos ao redor do mundo nas últimas décadas. Dois novos conceitos são incorporados às políticas de inclusão digital: a acessibilidade de todas as TIs (e-Accessibility), neste caso, não somente à população deficiente, mas também dar a competência necessária de uso das novas tecnologias para pessoas e assim incorporá-las à sociedade da informação (e-Competences).

UNIDADE 3

Princípios De Telecomunicações (Parte I)

Objetivo: Entender os princípios básicos que regem as Telecomunicações.

Qualquer tipo de comunicação ocorre quando a informação é transmitida (ou enviada) entre uma fonte de informação e o usuário que requisitou essa informação. Para que a informação seja transferida de um ponto a outro, deve existir um meio ou canal de transmissão entre a fonte e o receptor. As três partes, transmissor, canal e receptor representam assim o sistema de informação completo.

O sistema mais simples de comunicação é quando existe a conversação entre duas pessoas, nesse cenário básico vamos supor que as duas pessoas estão se afastando uma da outra. Neste caso, a pessoa que faz de fonte começa a elevar a voz para que a outra pessoa possa ouvi-la, porém existirá um ponto em que não será mais possível ouvir a fala da outra pessoa mesmo que ela esteja gritando com toda força. Para que continue a existir uma comunicação entre as duas pessoas será necessária a ajuda de dispositivos que permitam o envio da fala entre elas, mas essa informação falada deve ser previamente processada (pelos dispositivos) antes de ser enviada pelo canal de transmissão.

Portanto, essa informação falada deve ser colocada em um formato (linguagem) que é compreensível por máquinas, neste caso diz-se que a informação foi convertida em dados. A transmissão de dados ocorre quando estes são transferidos eletronicamente entre as duas pessoas. E assim, a conversação entre elas continuará a existir surgindo então, o conceito de comunicação à distância ou telecomunicação.

O sistema eletrônico de informação resultante pode ser um sistema de telemetria, um sistema digital de computação, um sistema de telefonia ou TV, etc. Em todos os casos estamos perante um sistema de telecomunicações.

Comutação Nas Redes De Telecomunicações

A função de comutação, ou chaveamento, em um sistema de comunicações trata da alocação dos recursos (meios de transmissão, repetidores, sistemas intermediários, etc.) do sistema para a transmissão de dados pelos diversos dispositivos conectados.

Quanto ao tipo de comutação utilizado, poderemos classificar as redes de Telecomunicações em três tipos:

- Comutação de Circuitos
- Comutação de Pacotes
- Comutação de Mensagens

Comutação De Circuitos

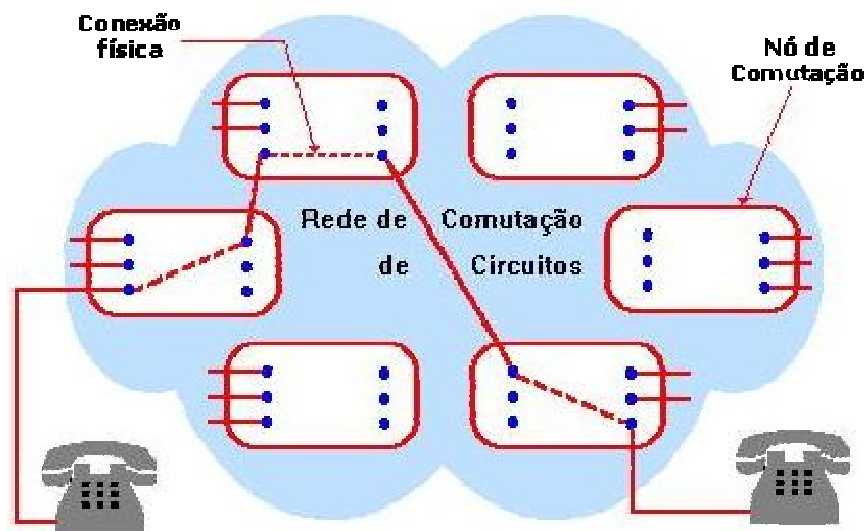
Nas redes de comutação de circuitos, antes de ser enviada qualquer informação, procede-se ao estabelecimento de um “caminho físico" ponta a ponta entre os terminais que pretendem estabelecer a comunicação, em outras palavras, deve previamente existir uma conexão física entre os usuários pela qual a informação deverá ser transmitida. A comunicação via comutação de circuitos envolve três etapas:

1) Estabelecimento da conexão;
2) Transferência da informação;
3) Desconexão do circuito.

Portanto, na comutação de circuitos os recursos do sistema são alocados para estabelecer a conexão, mantendo-se alocados até que a conexão seja desfeita, em outras palavras, entre os nós de Transmissão e Recepção (e vice-versa), um canal (circuito) físico é totalmente

dedicado até a finalização da conexão onde esse circuito é desfeito e passa a ser liberado para que outros usuários (da rede telefônica) possam fazer uso dele.

O caminho dedicado entre a origem e o destino pode ser:

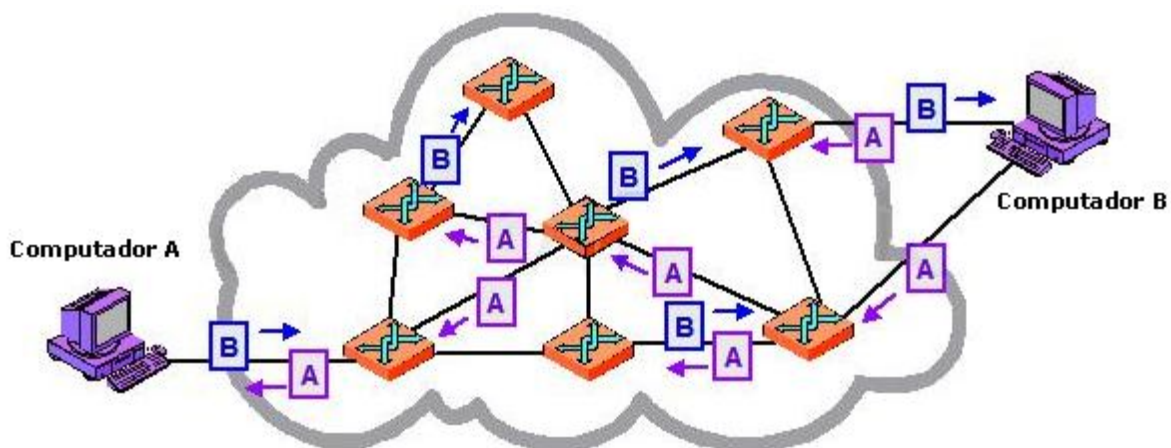
- Um caminho físico formado por uma sucessão de enlaces ou conexões físicas;
- Uma sucessão de canais de frequência, como nos sistemas FDMA (Frequency Division Multiple Access), isto é, canais com acesso múltiplo por divisão de frequência, alocados em cada enlace ou conexão física.
- Uma sucessão de canais de tempo, como nos sistemas TDMA (Time Division Multiple Access), alocados em cada enlace (ou conexão), sendo bastante utilizada nos atuais sistemas telefônicos para as ligações telefônicas comuns.

Comutação De Mensagens

A comutação de mensagens é um segundo tipo de comutação possível nas redes de telecomunicações. Nestas redes de comutação de mensagens não existe um caminho físico pré-estabelecido entre o emissor e o receptor.

Na comutação de mensagens a estação adiciona o endereço de destino da mensagem e transmite esta mensagem (completa) de nó em nó, em um processo conhecido como Store-and-Forward, ou seja, traduzindo do inglês, algo assim como armazenar (temporariamente a mensagem recebida) e logo enviá-la ou encaminhá-la para o seguinte nó. As mensagens só seguem para o nó seguinte após terem sido integralmente recebidas do nó anterior e assim sucessivamente até chegar ao destino final. Por tal motivo, cada nó deve ter uma capacidade considerável de armazenamento para poder temporariamente segurar a mensagem.

Um exemplo típico deste tipo de redes é o serviço de Correio Eletrônico X.400, por exemplo, das redes X.25.

Comutação De Pacotes

No contexto de redes de computadores, a comutação de pacotes é um paradigma de comunicação de dados em que pacotes (unidade de transferência de informação) são individualmente encaminhados entre nós da rede através de conexões tipicamente compartilhadas por outros nós. Este contrasta com o paradigma rival, a comutação de circuitos, que estabelece uma ligação virtual entre ambos os nós para seu uso exclusivo durante a transmissão (mesmo quando não há nada a transmitir). A comutação de pacotes é utilizada para otimizar a largura de banda da rede, minimizar a latência (i.e., o tempo que o pacote demora a atravessar a rede) e aumentar a robustez da comunicação.

Nesta técnica a transmissão da informação é dividida em envelopes de dados discretos, denominados pacotes. Desse modo, em caso de falha durante a transmissão, a informação perdida afeta uma fração do conteúdo total, em vez de afetar o todo. A estação receptora encarrega-se de montar os pacotes recebidos na sequência correta para reconstruir o arquivo (mensagem) enviado.

A grande diferença em relação à comutação de mensagens é que na comutação por pacotes, por ser cada pacote menor que a mensagem, o atraso de transmissão total da mensagem é reduzido. Redes com comutação de pacotes requerem nós de comutação com menor capacidade de armazenamento e procedimentos de recuperação de erros mais eficientes do que para comutação de mensagens.

A comutação de pacotes é mais complexa, apresentando maior variação na qualidade de serviço, introduzindo Jitter1 e atrasos vários; porém, utiliza melhor os recursos da rede, uma vez que são utilizadas técnicas de multiplexação temporal estatística.

A comutação por pacotes pode efetuar-se:

- Com ligação (circuito virtual): É estabelecido um caminho virtual fixo (sem parâmetros fixos, como na comutação de circuitos) e todos os pacotes seguirão por esse caminho. Uma grande vantagem é que oferece a garantia de entrega dos pacotes, e de uma forma ordenada. Exemplos: ATM (comutação de células), Frame Relay e X.25;
- Sem ligação (datagrama): Os pacotes são encaminhados de forma independente com números de sequência, oferecendo flexibilidade e robustez superiores, já que a rede pode reajustar-se mediante a quebra de um enlace de transmissão de dados. É necessário enviar-se sempre o endereço de origem. Ex: endereço IP.

---

[1] Basicamente o Jitter é a variação estatística do retardo na entrega dos pacotes de dados em uma rede.

Formato Das Mensagens

Os dados transportados por uma rede de computadores devem conter, no mínimo, as seguintes partes:

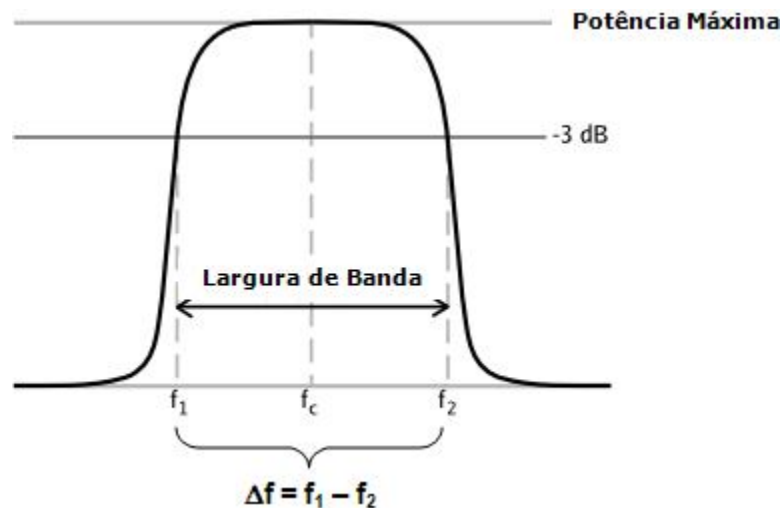
- Bytes de sincronismo (no início do quadro);
- Um identificador (endereço) dos dados;
- Campos de controle que implementam o protocolo, isto é, mensagens de movimento de dados na rede;
- Dados do usuário (do processo de aplicação);
- Um elemento para verificar erros de transmissão, normalmente denominado como campo de verificação de erros, ou campo de sequência de quadro FCS (Frame Check Sequence) posicionado tipicamente no final do quadro;

Largura De Banda

A largura (ou comprimento) de banda é a característica física de um sistema de telecomunicações que indica a velocidade na qual a informação pode ser transmitida em um determinado instante de tempo pelo canal de informação (par trançado, radiofrequência, ou fibra óptica). Em sistemas analógicos, mede-se em ciclos por segundo (Hertz) e em sistemas digitais em bits por segundo (bps).

Em radiocomunicação ela corresponde à faixa de frequências ocupada pelo sinal modulado sem sofrer distorção, isto é, corresponde à faixa de frequências na qual um sistema de comunicações tem uma resposta aproximadamente plana (com variação inferior a 3db), na região $\Delta f = f2 - f1$ a potência do sinal modulado é máxima.

A transmissão de grande quantidade de informação, em um intervalo pequeno de tempo, necessita sistemas de banda larga para acomodar os sinais. Uma utilização eficiente de um sistema exige a minimização do tempo de transmissão, para permitir o envio do máximo de

informações no menor tempo possível. A largura de banda representa uma limitação em sistemas de comunicação. Se a banda for insuficiente, poderá ser necessário diminuir a velocidade de sinalização aumentando o tempo de transmissão.

Podemos comparar a largura de banda como uma estrada. Esta estrada representa a conexão de rede e os carros são os dados. Quanto maior (mais ampla) for a estrada mais carros circularão por ela e consequentemente mais carros chegarão a seus destinos mais rápido. O mesmo principio pode ser aplicado aos dados transmitidos por um canal, quanto maior a largura de banda deste, maior o volume de dados transmitidos por intervalo de tempo.

Capacidade De Canal

A capacidade de canal é a propriedade de um determinado canal físico sobre o qual a informação é transmitida. Porém agora devemos interpretar com cuidado o que é um canal. O canal significa não somente o meio físico (cabos, ondas de rádio, etc.) de transmissão, mas também no conceito do canal devem ser incluídas as seguintes especificações:

- Os tipos de sinais transmitidos, isto é, se os sinais são binários (com dois níveis só 0s ou 1s) ou com M-níveis de codificação (neste caso temos os sinais M-ary), ou outro tipo de sinal.

- O tipo de receptor utilizado (o receptor determina a probabilidade de erro).

Todas estas especificações devem ser incluídas no conceito de Capacidade de Canal. Por exemplo, decidimos utilizar uma codificação de 4-ary dígitos em lugar de dígitos binários para enviar informação digital sobre um mesmo canal físico, evidentemente que com símbolos 4-ary a quantidade de informação enviada dobrará do que com dígitos binários. Vejamos o porquê disto:

Sistemas De Comunicação Digital M-Ary

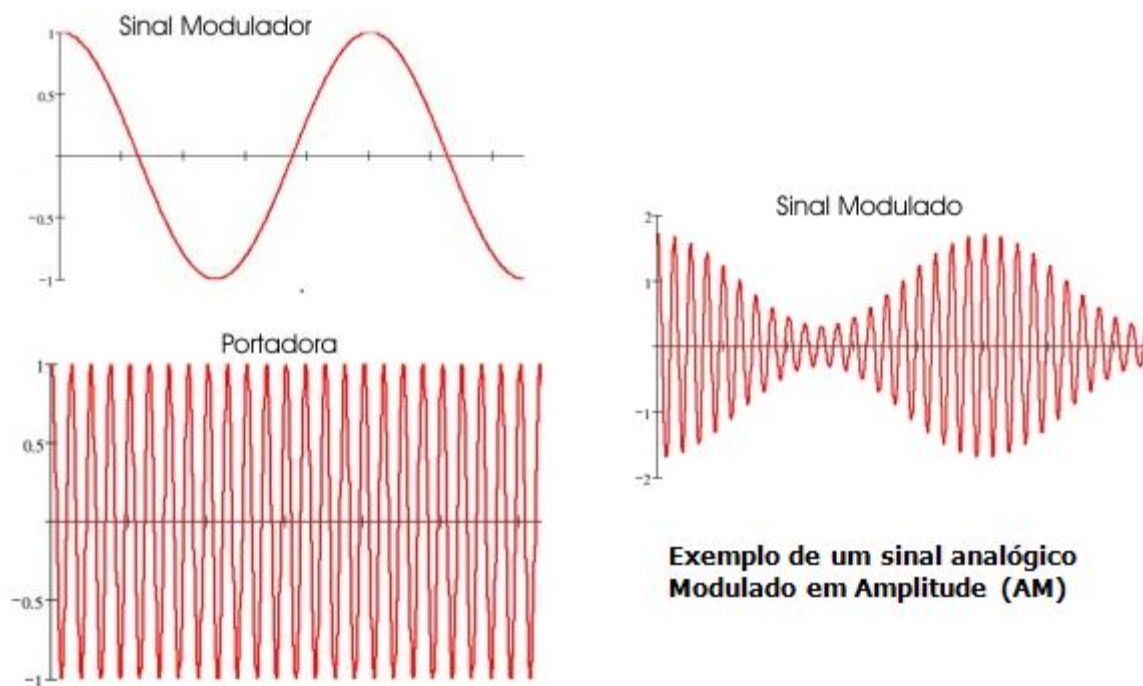
Normalmente a comunicação digital utiliza um número finito de símbolos entre o receptor e o transmissor, sendo o número mínimo igual a dois símbolos (o caso binário 0s e 1s). Mas existem os sistemas de comunicação digital com M símbolos (M-ary Comunication Systems), onde $M = 2^n$ com n sendo o número de bits a serem transmitidos por cada símbolo M.

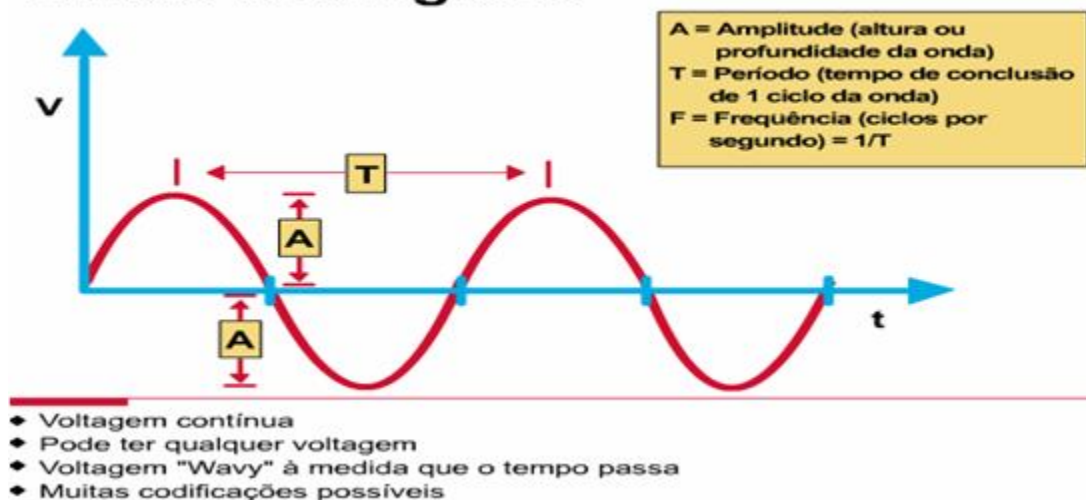
Por exemplo, se escolhermos n = 2 bits, então teríamos $M = 2^2 = 4$ símbolos, isto significa que para cada dois bits de informação basta transmitir um único símbolo 4-ary, duplicando assim a capacidade de transmissão. Se escolhermos n = 3 bits, então $M = 2^3 = 8$ símbolos, ou seja, um único símbolo 8-ary permitiria o envio de 3 bits. Com n = 4 bits, podemos lograr o envio de $M = 2^4 = 16$ símbolos e assim sucessivamente.

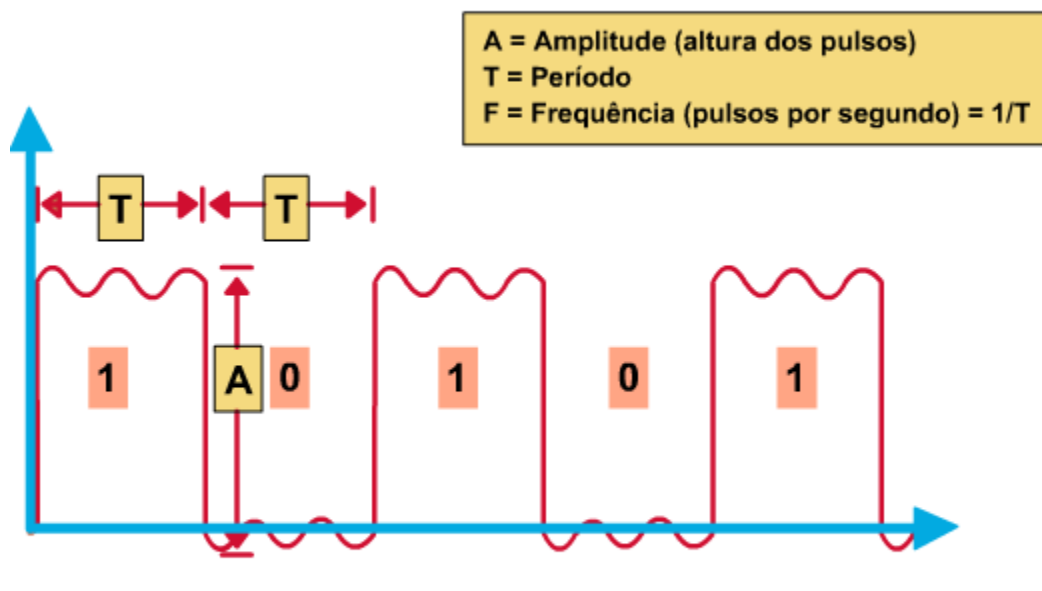
Em resumo quanto maior o número de símbolos (níveis) M-ary maior será a capacidade de canal para transmitir a informação digital, em outras palavras, pode-se incrementar a velocidade (taxa) de transmissão da informação incrementando o número de símbolos (ou níveis de codificação) M. Obviamente o custo de utilizar transmissores e receptores suportando níveis de codificação (M-ary) cada vez maiores será elevado.

Modulação

É interessante notar que muitas formas não elétricas de comunicação, também envolvem um processo de modulação, como a fala, por exemplo. Quando uma pessoa fala, os movimentos da boca são realizados a taxas de frequências baixas, da ordem de 10 Hertz, não podendo a esta frequência produzir ondas acústicas propagáveis. A transmissão da voz através do ar é conseguida pela geração de tons portadores de alta frequência nas cordas vocais, modulando estes tons com as ações musculares da cavidade bucal. O que o ouvido interpreta como fala é, portanto, uma onda acústica modulada, similar, em muitos aspectos, a uma onda elétrica modulada.

Exemplo de um sinal analógico Modulado em Amplitude (AM)

Em um sistema de transmissão de dados, seja este digital ou analógico, com ou sem-fio, é extremamente necessário utilizar métodos de inserir a informação útil que desejamos transmitir dentro de um sinal de Radiofrequência (RF), chamado de onda portadora (Carrier), que será o veículo de transporte da informação de um ponto a outro. Estes métodos de poder inserir a informação dentro de um sinal de RF são conhecidos como modulação da

onda portadora. Estes métodos de modulação permitem que a informação que queremos enviar seja transportada (embutida) já seja nos parâmetros de amplitude, frequência ou fase da onda portadora.

Nos sistemas de modulação digital, os bits do sinal de informação são codificados através de símbolos. A modulação é responsável por mapear cada possível sequência de bits de um comprimento preestabelecido em um símbolo determinado. O conjunto de símbolos gerado por uma modulação é chamado de constelação, sendo que cada tipo de modulação gera uma constelação de símbolos diferentes. Os símbolos nos quais as sequências de bits de um sinal de informação são transformadas é que serão transmitidos pela onda portadora.

Normalmente quando enviamos informação digital por linhas analógicas o processo de modulação converte os bits de informação em sinais analógicos para que possam ser enviados corretamente pelo canal de comunicação. No lado do receptor o processo de demodulação faz exatamente o contrário, isto é, os sinais analógicos são processados para serem transformados novamente em bits de informação. O equipamento que realiza a modulação e demodulação é denominado MODEM (MOdulação/DEModulação).

Técnicas Básicas de Modulação Analógica

Existem três técnicas para a modulação de sinais analógicos, a saber:

1. Modulação em amplitude (AM),
2. Modulação em frequência (FM) e
3. Modulação em fase (PM).

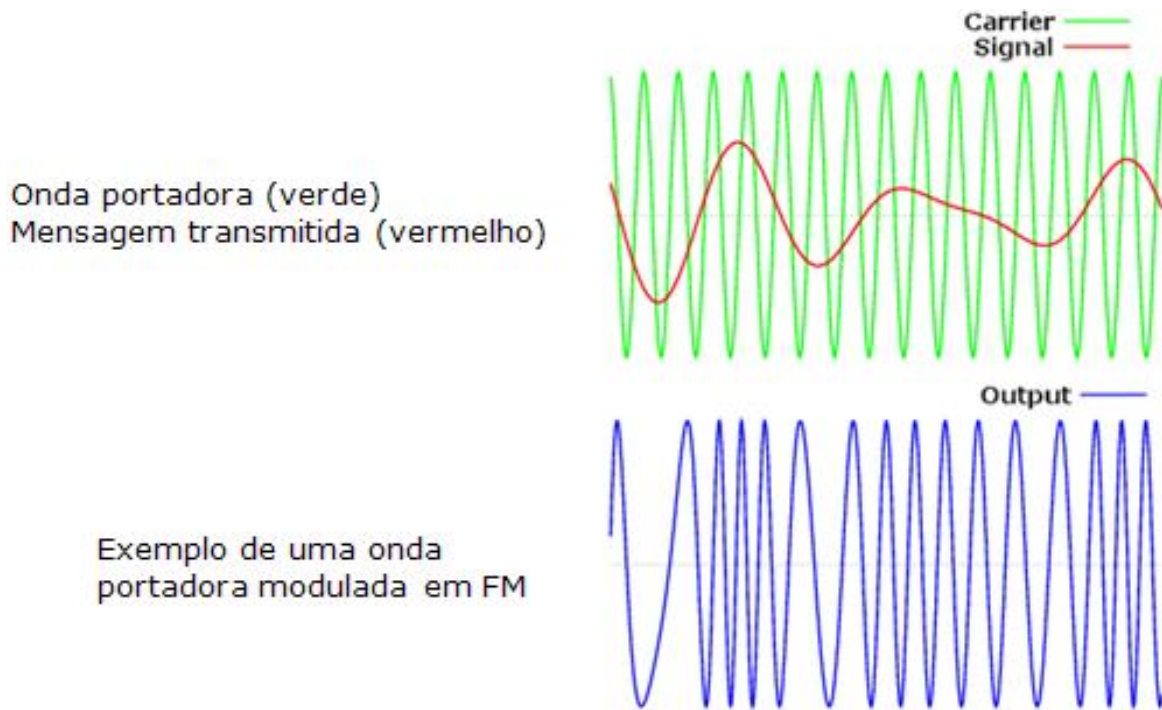
Modulação Em Amplitude AM (Amplitude Modulation)

A modulação AM é a forma de modulação em que a amplitude da onda portadora (sinal verde na figura) varia em função do sinal modulador (sinal vermelho na figura), o sinal modulador é o sinal que contem a nossa informação, ou seja, o sinal modulador é a informação desejada (ou informação útil) que estamos transmitindo. Nesta técnica de modulação AM, tanto a frequência como a fase da onda portadora são mantidas constantes, como pode ser visualizado na onda (sinal) de saída dada pelo sinal azul na figura. Este último sinal (em azul) é o sinal que é enviado pelo ar até os receptores, por isso é que se denomina sinal de saída (Output) do transmissor.

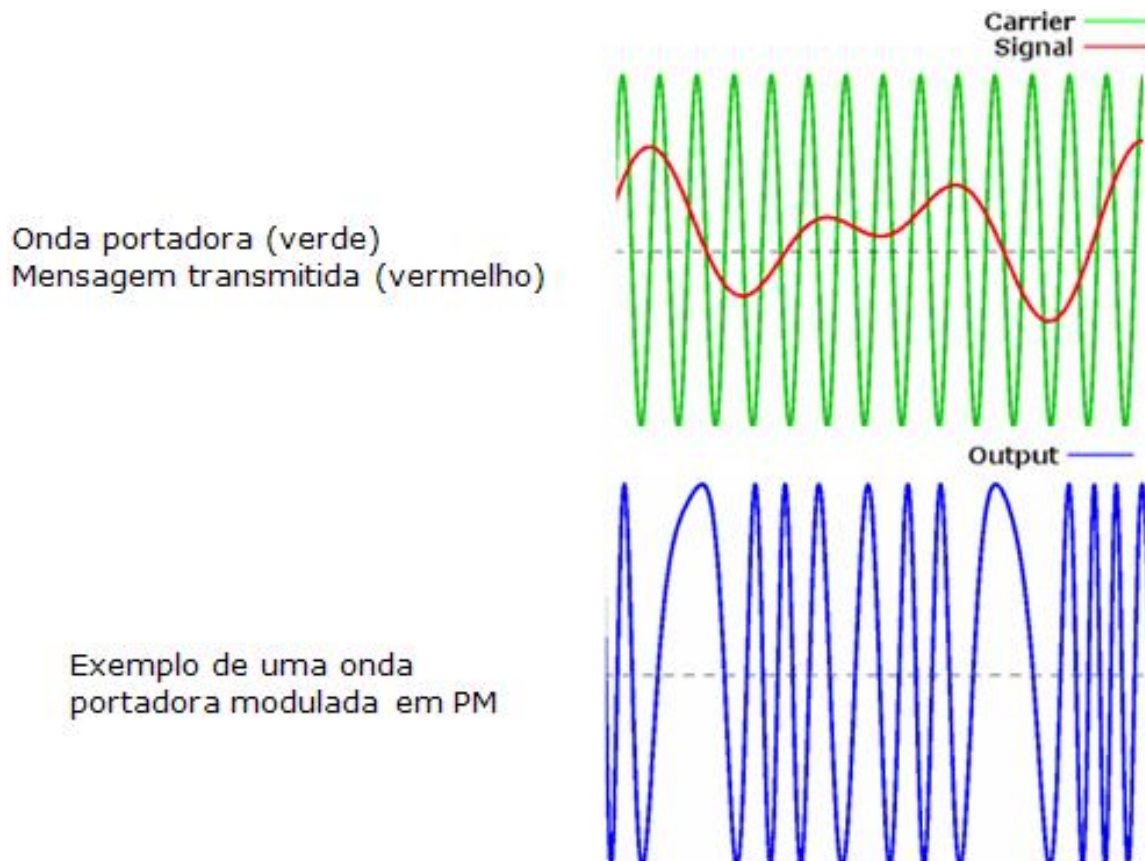
Modulação Em Frequência FM (Frequency Modulation)

Agora se em lugar de variar a amplitude, o sinal modulador variar a frequência da portadora, pode-se esperar uma melhor qualidade de transmissão, uma vez que a frequência do sinal não é afetada por interferências. A contrapartida para a melhor qualidade da FM é uma largura de banda maior. No caso de estações de rádio, enquanto uma transmissão de AM pode ser razoavelmente efetuada numa faixa de 10 kHz, uma de FM precisa de larguras tão altas como 150 a 200 kHz para uma boa qualidade.

Por isso, as frequências reservadas para transmissões comerciais de rádios de FM estão na faixa de frequências muito altas VHF (Very High Frequency), a faixa comercial das radioemissoras de FM vai desde os 88 MHz até os 108 MHz, nesta faixa (ainda) é possível acomodar um número razoável de estações de rádio (aproximadamente 90 emissoras).

Exemplo de uma onda portadora modulada em FM

Modulação Em Fase PM (Phase Modulation)

As técnicas de modulação FM e PM têm muitas características semelhantes. A modulação por fase é um tipo de modulação analógica que se baseia na alteração da fase da portadora de acordo com o sinal modulador (mensagem). A diferença da modulação FM, a modulação PM não é muito utilizada exceto, talvez, no (mal chamado) método FM Synthesis para instrumentos musicais, introduzido pela Yamaha por volta de 1982. Isto, principalmente, se deve ao requerimento de um equipamento (Hardware) bem mais complexo para seu processamento e também porque poderiam existir problemas de ambiguidades para determinar se, por exemplo, o sinal tem 0° de fase ou 180° de fase.

Pode-se observar na figura como a frequência do sinal de saída (sinal azul) diminui quando o sinal modulador (sinal vermelho) esta decrescendo, diferente da modulação FM onde a diminui justo quando o sinal modulador esta no seu ponto mínimo.

Técnicas Básicas De Modulação Digital

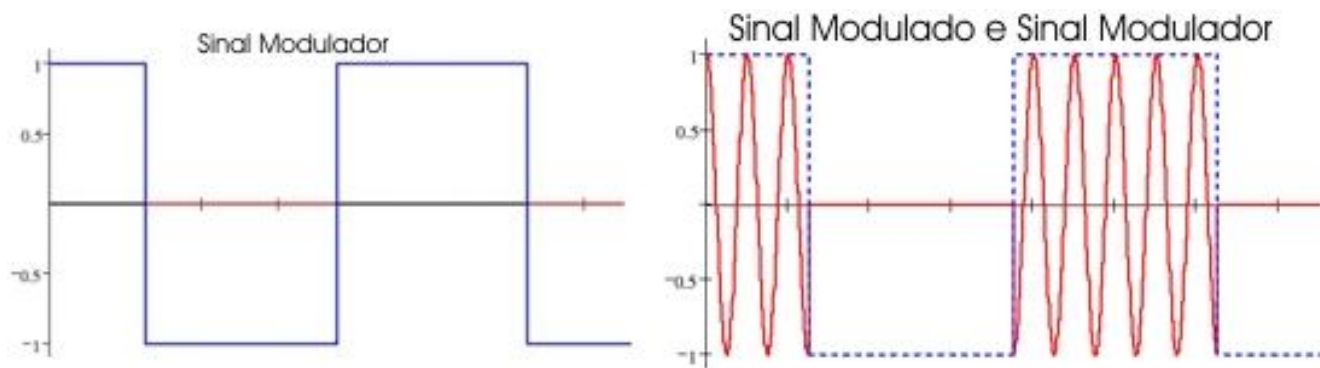
Também denominada modulação discreta ou codificada. Utilizada em casos em que se está interessado em transmitir uma forma de onda ou mensagem, que faz parte de um conjunto finito de valores discretos representando um código. No caso da comunicação binária, as mensagens são transmitidas por dois símbolos apenas. Um dos símbolos representado por um pulso S(t) correspondendo ao valor binário "1" e o outro pela ausência do pulso (nenhum sinal) representando o dígito binário "0".

Como se pode observar, os bits possuem estados bem definidos (1 ou 0) e por esta razão não podem ser transmitidos (irradiados) com eficiência como um sinal senoidal. Os processos de modulação digital consistem em modular uma informação binária através de uma onda portadora analógica senoidal, utilizando as mesmas técnicas da modulação analógica.

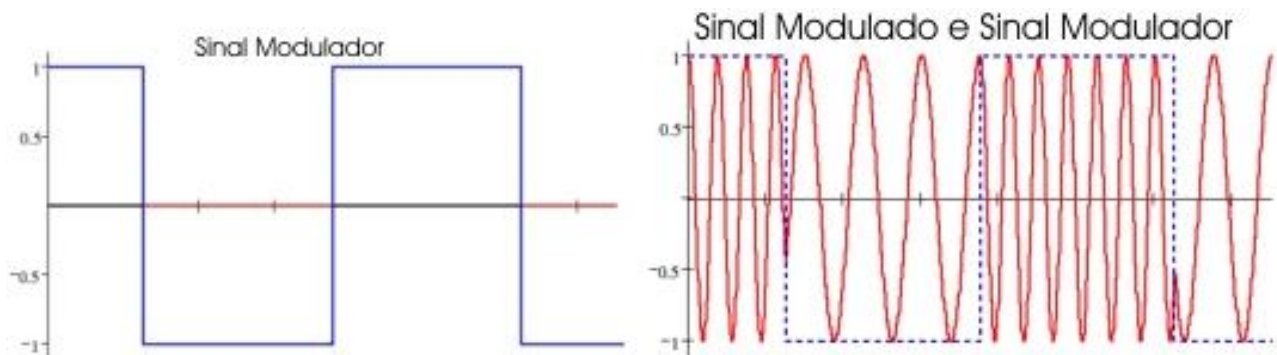
A diferença fundamental entre os sistemas de comunicação de dados digitais e analógicos (dados contínuos) é bastante óbvia. No caso dos dados digitais, envolve a transmissão e detecção de uma dentre um número finito de formas de onda conhecidas (no presente caso a presença ou ausência de um pulso), enquanto que, nos sistemas contínuos há um número infinitamente grande de mensagens cujas formas de onda correspondentes não são todas conhecidas.

No caso específico do sinal modulador ser um sinal digital, essas técnicas de modulação analógica, vistas anteriormente, tomam as seguintes denominações:

Modulação ASK (Amplitude Shift Keying)

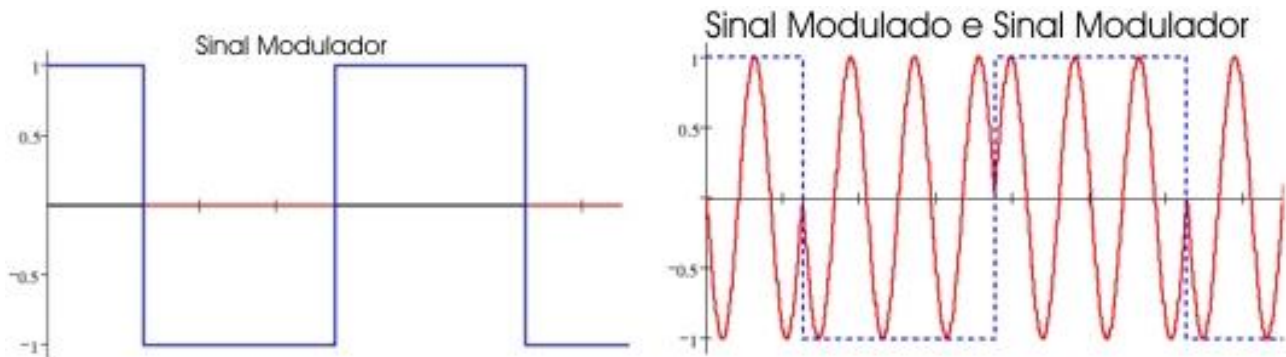
A técnica de modulação ASK (ou modulação por chaveamento da amplitude) é também conhecida como a modulação On-Off, ASK é o método mais simples de modulação digital. Consiste na alteração da onda portadora em função do sinal digital a ser transmitido. A onda resultante consiste então em pulsos de radiofrequência, que representam o sinal binário 1 e espaços representando o dígito binário 0 (supressão da portadora).

Daí o nome de On-Off porque pareceria que a onda portadora é ligada e desligada dependendo do valor dos bits de informação enviados. Atualmente esta técnica não é mais utilizada em sistemas de transmissão digital.

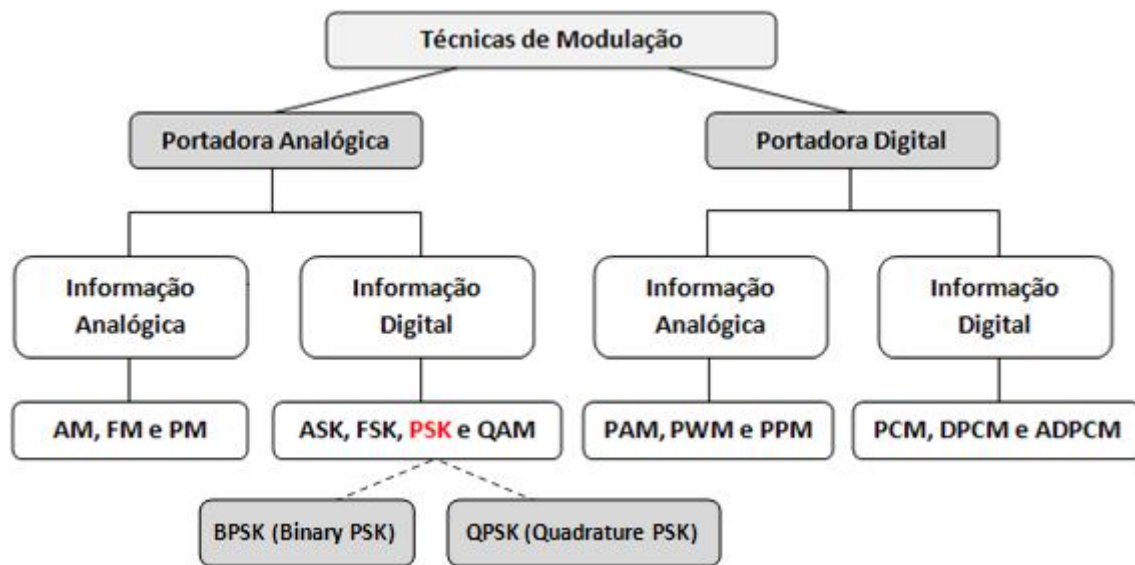
Modulação FSK (Frequency Shift Keying)

O processo de modulação FSK (ou modulação por chaveamento da frequência) consiste em variar a frequência da onda portadora em função do sinal modulador, no presente caso, o sinal digital a ser transmitido. Este tipo de modulação pode ser considerado equivalente à modulação em FM para sinais analógicos.

A amplitude da onda portadora modulada é mantida constante durante todo o processo da modulação; quando ocorrer a presença de um nível lógico "1" no sinal digital, a frequência da portadora é modificada para uma frequência f_1, e para um valor 0 a frequência da portadora muda para um valor f_2 estas mudanças de frequências podem ser depois compreendidas no processo de demodulação.

Modulação PSK (Phase Shift Keying)

A técnica PSK (ou modulação por chaveamento da fase) é o processo pelo qual se altera a fase da onda portadora em função do sinal digital a ser transmitido. Quando ocorrer uma transição de nível lógico do sinal digital a ser transmitido (sinal modulador), haverá uma mudança de 180° graus na fase da onda portadora com relação à fase anterior.

A transição de fases observada pode ser tanto de nível lógico 0 para 1 como de nível lógico 1 para 0. Para este tipo de modulação deve ser utilizada a detecção síncrona, já que esta tem como base o conhecimento preciso a respeito da fase da onda portadora recebida, bem como da sua frequência. Esta técnica de modulação devido ao fato mencionado envolve circuitos de recepção (demodulação) mais sofisticados; em compensação oferece melhor desempenho que as técnicas ASK e FSK. Por tal motivo a modulação PSK é bastante utilizada em sistemas de telecomunicações.

Resumo dos Tipos de Modulação

O quadro a seguir apresenta um resumo dos diferentes tipos de modulação utilizando tanto uma onda portadora analógica ou digital e a informação enviada analógica ou digital.

Demodulação

É o processo que nos permite reverter o processo da modulação. Também chamado de detecção, envolve dispositivos eletrônicos, chamados modems, encarregados de detectar a onda portadora modulada e extrair dela o sinal modulante (a informação desejada).

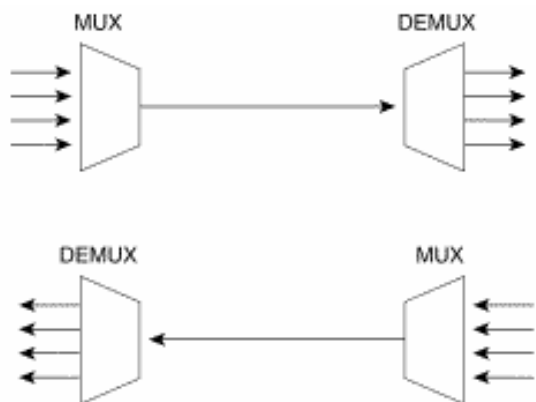
No processo da demodulação para sinais digitais, a forma de onda não é importante, pois ela já é conhecida. O problema se resume a determinar se o pulso está presente ou ausente, portanto, o ruído do canal não tem influência nesse sentido. Entretanto o ruído do canal poderá causar certos erros nas decisões. A decisão na detecção pode ser facilitada com a passagem do sinal através de filtros que reforçam o sinal útil e suprimem o ruído ao mesmo tempo. Isso permite melhorar muito a relação Sinal/Ruído reduzindo a possibilidade de erro.

Nos sistemas digitais o problema da detecção (demodulação) é um problema um pouco mais simples que nos sistemas contínuos. Durante a transmissão, as formas de onda da onda portadora modulada são alteradas pelo ruído do canal. Quando este sinal é recebido no receptor, devemos decidir qual das duas formas de onda possíveis conhecidas foi

transmitida. Uma vez tomada a decisão a forma de onda original é recuperada sem nenhum ruído.

Multiplexação

Um dos maiores problemas na implementação de uma rede de comunicação de dados é o alto custo das linhas de comunicação. Por isso há a necessidade de otimizar estas linhas. Por exemplo, se cada estação de trabalho possuir uma linha direta ao servidor, a atividade média nesta linha será excessivamente baixa, devido a períodos inativos longos com nenhum ou pouquíssimo fluxo de dados. Se existem períodos ativos entre as várias linhas que nunca coincidem, é possível comutar uma única linha para atender os vários terminais.

Mas existe a possibilidade de mais de um terminal estar ativo em determinado instante, e se não existem regras para as estações ligadas ao comutador surgirá um conflito na linha gerando um grave problema. Este problema pode ser resolvido fazendo com que a linha que sai do comutador seja maior do que qualquer linha de entrada, sendo assim a linha de saída é maior que a soma das linhas de entrada eliminando o problema.

Sistemas MUX/DEMUX unidirecionais

Sistema MUX/DEMUX bidirecional

Com isso o comutador executa a função de multiplexador. O multiplexador (MUX) é um dispositivo cuja função é permitir que múltiplas estações de trabalho possam compartilhar

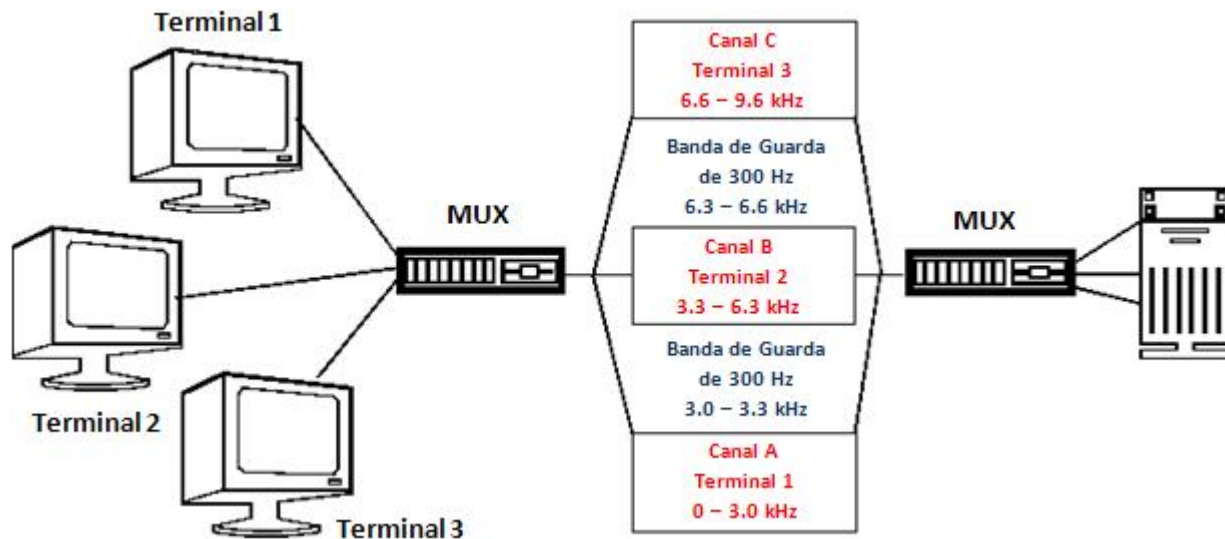
uma linha de comunicação. Do lado oposto encontra-se o demultiplexador (DEMUX) que faz o processo contrário distribuindo os sinais desde o canal principal para os respectivos canais secundários.

Portanto, em um sistema unidirecional, existe um MUX na transmissão e um DEMUX na recepção. Dois sistemas são necessários para uma comunicação bidirecional, cada um com seu próprio canal principal de comunicações. Em um sistema bidirecional, existe um MUX/DEMUX em cada terminação, sendo a comunicação realizada por um único par de cabos (para trançado, coaxial, fibras). É fundamental nestes dispositivos minimizar o efeito “Cross-Talk” e maximizar a separação de canais.

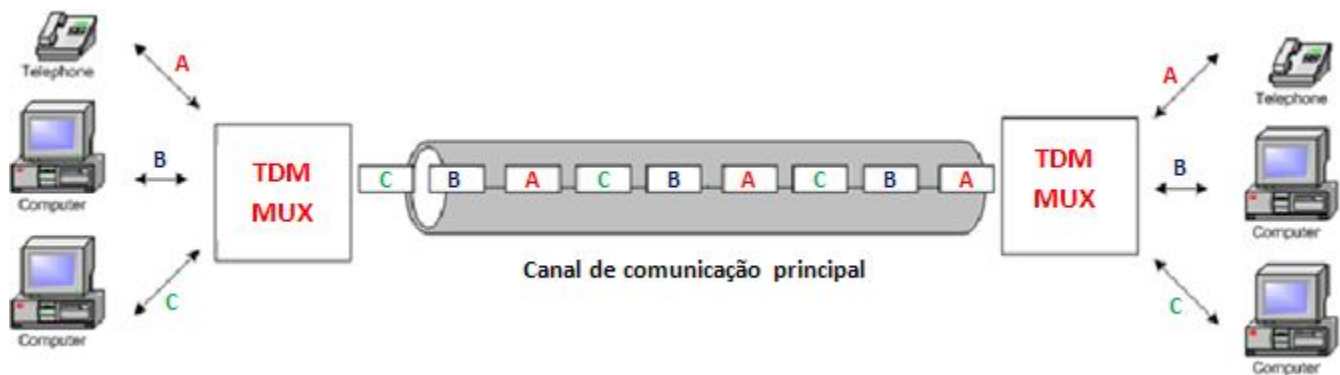
O canal principal tem capacidade (largura de banda) suficiente para suportar o uso compartilhado pelos canais secundários. Com isso, os multiplexadores reduzem o número de linhas de comunicação necessárias, conseguindo uma redução nos custos, pois diminuem o cabeamento necessário.

O processo de multiplexação (ou multicanalização) se divide em: Multiplexação por divisão de frequência (FDM), multiplexação por divisão de tempo (TDM) e multiplexação estatística por divisão de tempo (STDM).

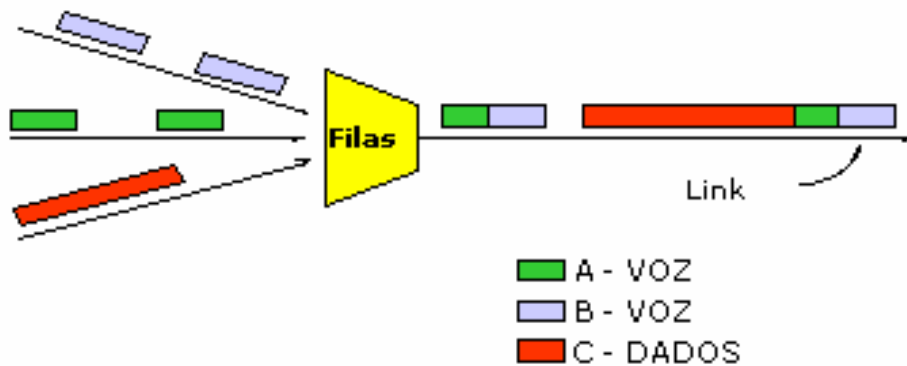
FDM (Frequency Division Multiplexing)

Na técnica de multiplexação por divisão de frequência, a largura de banda da linha principal de comunicações é dividida em várias frequências com isso surgem várias bandas mais estreitas, e cada terminal tem acesso a uma, ou seja, esta técnica permite transmitir simultaneamente vários canais (sinais), através de um único canal físico (meio de transmissão), onde cada sinal de usuário (canal secundário de comunicação) possui uma banda espectral (frequência) própria e bem definida, que, em condições normais de funcionamento é bem menor que a largura de banda total da linha (canal) de comunicação principal.

TDM (Time Division Multiplexing)

Esta técnica da multiplexação por divisão de tempo intercala os bits, que fluem das linhas de baixa velocidade entrantes para dentro da linha saída de alta velocidade. Em ambos os métodos o resultado é que uma única linha de alta velocidade transmite de forma serializada um número de sinais (canais) de entrada com velocidades mais baixas.

Portanto, a técnica TDM permite transmitir simultaneamente vários canais (sinais), dentro do mesmo canal físico (meio de transmissão), onde cada sinal de usuário (canais de comunicação secundários A, B e C da figura) possui uma janela de tempo próprio e definido de uso da banda para transmissão.

No caso desta técnica TDM o uso da largura de banda (da linha de comunicações principal) poderia não ser ótimo, sobre todo quando poderiam existir canais de usuários que não estejam transmitindo nada, já que essa janela de tempo não estaria sendo temporariamente utilizada por ninguém, portanto, desperdiçando banda, mas o ponto a favor é que a qualidade de serviço é elevada por termos uma banda garantida para cada usuário.

STDM (Statistical TDM)

A técnica de multiplexação estatística por divisão de tempo ou simplesmente multiplexação estatística é uma técnica muito útil quando se quer fazer um melhor uso da largura de banda total do canal principal de comunicações. Nesta técnica somente uma parcela de tempo é alocada se (e somente se) existir tráfego, ao contrário da TDM, e com isso se evita a má utilização da linha principal. Neste caso temos um uso aprimorado da largura de banda, mas poderia não existir uma qualidade de serviço no atendimento como é o caso do sistema TDM, já que a banda não necessariamente seria garantida para todos os usuários e certas demoras poderiam ser verificadas durante a transmissão e/ou recepção de dados

Obs.: Se o tráfego na linha é uniforme, então é mais vantajoso o uso da tecnologia TDM, que proporciona uma melhor utilização da capacidade da linha.

FDM x TDM

Na multiplexação por divisão de frequência (FDM) cada subcanal com determinada frequência é atribuída a cada um dos componentes do grupo, sendo assim pode se tornar difícil a expansão neste método visto que a adição de subcanais precisará de uma reatribuição de frequências.

Na multiplexação por divisão de tempo (TDM), como o tempo é dividido entre os terminais, o multiplexador examina as linhas de baixa velocidade em uma ordem pré-definida, e a linha de alta velocidade possui apenas um único sinal em um determinado instante. Isto difere da FDM, na qual, vários sinais são enviados ao mesmo tempo, porém cada um com uma diferente frequência. Normalmente a FDM é usada para sinais analógicos e a TDM com sinais digitais.

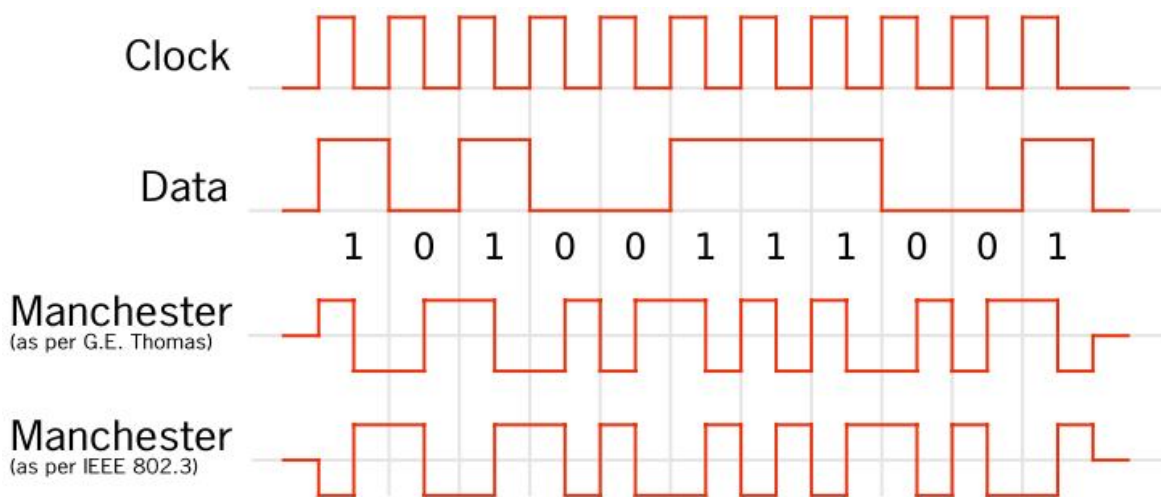
Para separar as frequências alocadas com a tecnologia FDM utiliza-se de guardas-de-banda. Na tecnologia TDM a separação das fatias de tempo é obtida com espaços de tempo entre quadros sucessivos de amostras completas de todos os canais. No caso da tecnologia TDM tem-se a TDM síncrona e a TDM assíncrona, que veremos mais adiante.

Sincronização

O processo de sincronização é parte do protocolo de comunicação. A transmissão de dados por uma rede de computadores é serial, devido ao custo mais baixo, os bits que compõem um caractere são transportados um após o outro, utilizando apenas um canal. A sincronização entre o emissor e o receptor, é realizada através de um sinal, de modo que o receptor e o transmissor estejam sincronizados previamente antes dos dados enviados chegarem ao receptor, esse sinal de sincronismo mantém o receptor sincronizado com a cadeia de bits transmitida, desta forma os dados enviados não seriam perdidos em teoria.

Se os terminais estiverem próximos fisicamente, a sincronização pode ser feita através de um canal dedicado, que transmite um sinal de sincronização. Nas redes LAN Ethernet o sinal de sincronismo se encontra no próprio cabeçalho do quadro Ethernet. Agora, se os terminais estiverem fisicamente distantes, o uso de um canal dedicado se torna inviável e neste caso e necessário um sinal de sincronização que esteja incorporado no sinal transmitido, no modo código com autosincronismo (Self-clocking Code). Os melhores códigos para relógio são aqueles que alteram o estado da linha com relativa frequência, permitindo que o receptor possa continuamente se ajustar ao sinal enviado. Estes códigos são muito utilizados nas transmissões de dados utilizando redes WAN.

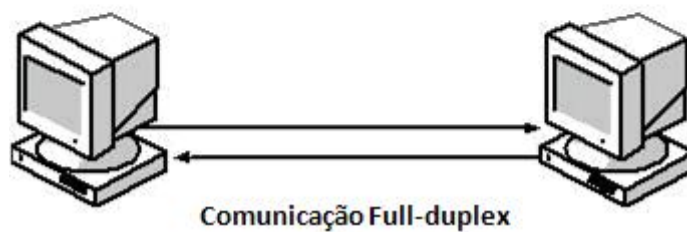
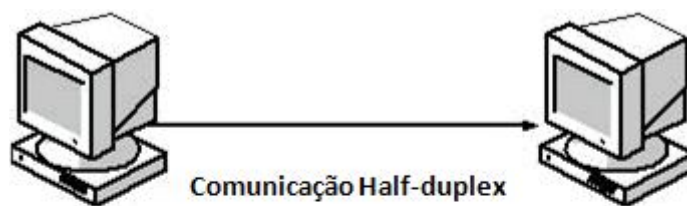
Em telecomunicações, um ótimo codificador de linha com sincronismo incluído (no próprio sinal transmitido) é o código Manchester, também conhecido como codificador Bifase (Biphase Encoder). Neste codificador de linha cada bit transmitido tem no mínimo uma transição e ocupa o mesmo intervalo de tempo, ou seja, um bit 1 é representado por uma transição positiva (subida) no meio do intervalo significativo do bit, enquanto o bit 0 corresponde a uma transição negativa (descida).

Pode-se observar que o codificador Manchester experimenta variações ao longo do tempo o que, por sua vez, produz um ótimo sinal de relógio (sincronismo) contido no sinal codificado, isto facilita muito ao receptor na hora de recuperar os dados.

O código Manchester é utilizado nas redes Ethernet. Existem códigos de linha mais complexos, por exemplo, os códigos 8B/10B o qual utiliza menos largura de banda para atingir a mesma taxa de transferência, mas que pode ser menos tolerante a erros de frequência e Jitter no relógio de referência (sinal de sincronismo) tanto do transmissor como do receptor.

Modos De Comunicação

O fluxo de dados em uma rede de comunicação pode ser realizado de três formas:

- **SIMPLEX**: O fluxo de dados ocorre em uma única direção. Utilizado pelas emissoras de TV e rádio difusão;
- **HALF-DUPLEX**: O fluxo de dados ocorre em ambas às direções, porém em uma direção de cada vez. Utilizado em sistemas do tipo Walk-talk;
- **FULL-DUPLEX**: O fluxo de dados ocorre em ambas às direções simultaneamente. Caracteriza-se alta vazão e utilização contínua de dados, diminuindo o tempo de resposta.

Comunicação Half-duplex
Comunicação Full-duplex

UNIDADE 4

Objetivo: Saber identificar os principais meios físicos de transmissão.

Princípios De Telecomunicações (Parte II)

Meios De Transmissão

O meio para a transmissão (da informação, dados) serve para oferecer suporte ao fluxo de dados entre dois pontos distantes. Usamos o termo linha para designar o meio de transmissão usado entre esses pontos. Essa linha pode ser constituída por um par de fios, um cabo coaxial, fibras ópticas, ou então pode ser um canal de comunicação por radiofrequência ou até mesmo por satélite. Aqui serão abordados os meios de transmissão mais comuns utilizados nos sistemas de comunicações.

Sistemas Por Rádio Enlace

Os sistemas de comunicações por radioenlace fazem uso do espectro eletromagnético, isto é, transmitem os dados através de ondas de radiofrequência (RF). Para que a transmissão de dados neste sistema tenha êxito é importante que certos requisitos sejam respeitados, a saber:

- Potência de transmissão;
- Mínima distorção na propagação do sinal;

As condições anteriores devem ser mantidas dentro de parâmetros suficientes para garantir a integridade dos dados transmitidos.

Por sua natureza, estes sistemas são adequados tanto para ligação ponto-a-ponto quanto para ligações multipontos. Seu emprego é particularmente importante para comunicações entre computadores e o ambiente de rede local móvel. A radiodifusão também é utilizada em aplicações onde à confiabilidade do meio de transmissão é um requisito indispensável.

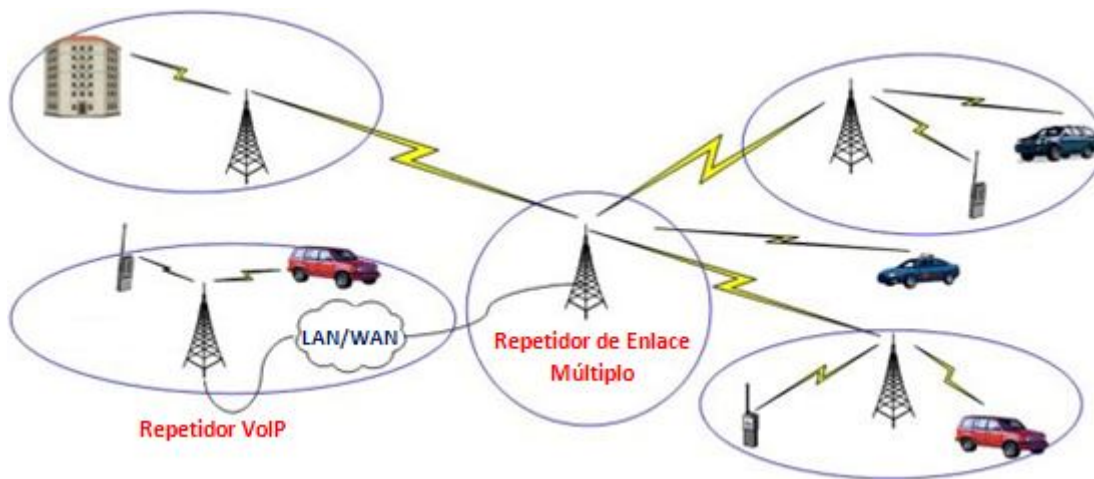
Nas ligações entre redes LAN, a radiodifusão também tem um papel relevante, especialmente se essas redes estão distantes e a taxa de fluxo de dados (entre elas) precisa ser elevada. Neste caso, circuitos telefônicos podem ser inadequados e a radiodifusão pode ter a largura de faixa exigida. Comunicações por luz infravermelha e micro-ondas são outros meios possíveis de comunicação.

A comunicação de dados utilizando um enlace de rádio com velocidades de 10 Mbps, 11 Mbps, 20 Mbps ou 100 Mbps está sendo uma das opções mais práticas e viáveis financeiramente para interligar redes locais Ethernet cujas distâncias não ultrapassem 30 km por enlace.

Por utilizar a tecnologia por espalhamento espectral (Spreed-Spectrum) na frequência de 2.4 Ghz ou 5.8 Ghz, a interligação dos locais onde estão instaladas as LANs dependerá de existir linha de visada direta entre as antenas de transmissão e recepção. Caso a topologia do local dificulte essa visada pela existência de obstáculos como prédios ou morros, podemos superá-los com o emprego de uma unidade repetidora localizada exatamente entre os pontos de conexão.

Se a distância entre os sites a serem conectados for superior a 4 km, será utilizado um amplificador de sinal de 1 Watt de potência para garantir a qualidade e sustentação do sinal entre as antenas transmissora e receptora.

A tecnologia Spread-Spectrum emprega um feixe de ondas de rádio na frequência de 915 MHz ou 2.4 GHz para a comunicação entre as antenas de transmissão e recepção. Esta tecnologia de espalhamento espectral reduz a sensibilidade a problemas atmosféricos como chuvas fortes, ruídos, campos eletromagnéticos e também a obstáculos naturais. Ao contrário da tecnologia de transmissão de dados via micro-ondas, onde os sinais são transmitidos sem espalhamento espectral entre as antenas o que torna a transmissão muito

mais susceptível a interferências atmosféricas, porém a tecnologia Spread-Spectrum se beneficia da largura (espalhamento) da banda (espectro) para obter uma conexão coerente dos sinais, mesmo em locais de difícil recepção. Um sistema comercial que utiliza esta técnica de Spread-Spectrum é o sistema de telefonia celular CDMA (Code Division Multiple Access).

Um enlace de rádio para tráfego Ethernet a 10, 11, 20 e 100 Mbps interliga duas redes locais consideradas as limitações de visada direta entre os pontos e distância máxima de 30 km. Em razão da performance e qualidade na transmissão, cada antena é conectada a um equipamento chamado “Bridge” (ponte) que transmite os quadros Ethernet que realmente precisam trafegar de uma rede para outra. Isso aumenta a disponibilidade e eficiência do link de rádio e reduz colisões nos barramentos das LANs.

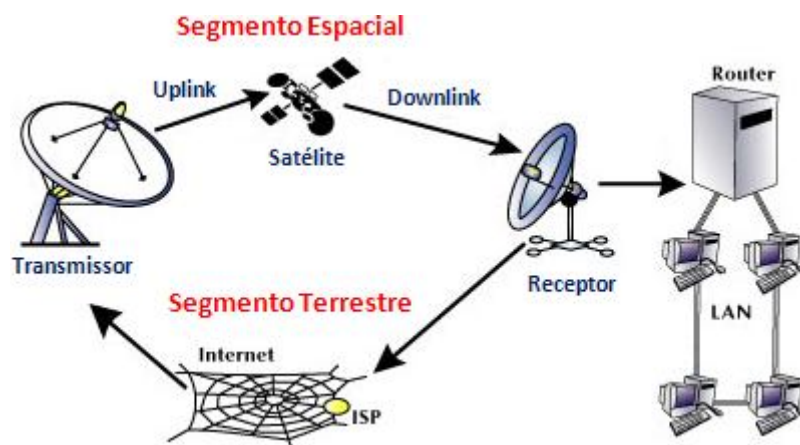
Redes LANs colocadas em edifícios distantes uns dos outros podem ser interligadas por canais com banda passante média de até 2 Mbps, uma taxa razoavelmente boa, e é possível transmitir (nessa velocidade) tanto dados tradicionais como imagens e até os canais de voz dos PABX (Private Automatic Branch Exchange) das empresas. No Brasil, usuários como Promom, EDS, Unibanco e a Marinha já trabalham com soluções de radiofrequência para suas redes LAN corporativas.

Sistemas Por Satélite

Sem dúvida alguma, o maior fator motivador para a utilização de satélites como meio de transmissão, é a inexistência de meios físicos entre localidades alvo da comunicação. Como os satélites podem cobrir praticamente quaisquer áreas do globo terrestre chegam a ser a melhor opção para atingir pontos de difícil acesso. Outro fato determinante para a utilização de satélites como meio de transmissão foi a indisponibilidade de meios de transmissão digital de baixo custo. As atuais redes digitais de alta velocidade não existiam há 15 anos atrás. Os serviços analógicos de transmissão, como o Transdata, apresentavam taxas de erro na ordem de 10^{-5}, contra 10^{-7} (ou menores) dos serviços digitais atuais.O custo dos meios de transmissão analógicos também foi um fator motivador para o uso da tecnologia satelital, tendo, todavia, deixado de ser, nos últimos anos.

O satélite é o elemento físico comum de interligação das estações terrenas, atuando como estação repetidora. Devido a sua altitude, permite a transmissão de sinais diretamente entre duas estações, sem que existam necessariamente pontos intermediários.

Um sistema via satélite está composto de um Segmento Espacial e um Segmento Terrestre:

- **O Segmento Espacial**: Composto por um ou mais satélites e pelos equipamentos necessários às funções de suporte e operação dos satélites, tais como telemetria, rastreio, comando, controle e monitoração.

- **O Segmento Terrestre**: São as estações terrenas de comunicação que transmitem os dados de um ponto geográfico para outro. Cada estação terrena está provista de uma antena parabólica, amplificadores de alta potência para transmissão (Uplink), amplificadores de recepção (Downlink) de baixo ruído e equipamentos de comunicação.

Dos vários subsistemas que um satélite possui o que mais nos interessa é o de comunicações. Neste sistema temos um repetidor ativo que recebe, converte a frequência, amplifica e retransmite para a Terra os sinais recebidos. Os circuitos são denominados Transponders. Cada Transponder é responsável pela recepção e retransmissão de uma determinada banda de frequência. Um satélite tem, tipicamente, de 20 a 40 Transponders.

As faixas de frequências utilizadas pelos sistemas satelitais são:

- **Banda L**: de 1,5 a 2,5 GHz
- **Banda C**: de 5,850 a 6,425 GHz (Uplink = Terra → Satélite)
  de 3,625 a 4,200 GHz (Downlink = Satélite → Terra)
- **Banda Ku**: de 14,0 a 14,5 GHz (Uplink = Terra → Satélite)
  de 11,7 a 12,2 GHz (Downlink = Satélite → Terra)
- **Banda Ka**: de 20,0 a 30,0 GHz

As bandas mais utilizadas são a **C** e a **Ku**, sendo a banda **Ku** a mais popular, isto devido às frequências mais altas que utiliza possibilitando assim o uso de antenas de menor tamanho. Mas tal vantagem é contrabalanceada por uma relevante característica em contra. A banda **Ku** sofre maior atenuação de sinal (pela chuva, por exemplo) em relação à banda **C**.

O Sistema Brasileiro De Transmissão Por Satélite (SBTS)

O SBTS de propriedade da Embratel é composto por satélites com as seguintes características básicas:

- Giroestabilizados: altitude é mantida pela força centrípeta da metade que gira sobre o próprio eixo;
- Comprimento 7,1 metros;
- Diâmetro 2,16 metros;
- Massa: 1.140 Kg (lançamento) e 671 Kg (órbita);
- Transponders: 36, 36 MHz/cada, 36 dBW;
- Redundância TWT ¼;
- Frequências de operação: 6,0 GHz (Uplink) e 4,0 GHz (Downlink);
- Energia: 982 W (inicial) e 799 W (final);
- Potência Irradiada (EIRP/canal): >= 34 dBW;
- Espectativa Vida Útil: 11 anos;
- Altitude: 36.000 km em 65W e 70W de potência (satélites Intelsat)

Existem diversos fornecedores de equipamentos para montagem de uma rede de transmissão via satélite, como Hughes, Vitacom, Tridom, Scientific Atlanta, NEC e G&E. O Segmento Espacial, no entanto, é provido apenas pela Embratel, no Brasil. Os serviços de provimento de facilidades via satélites chamam-se Serviços DataSat:

- **DataSat Plus**: Serviço SCPC/MCPC para transmissão em alta velocidade ponto-a-ponto ou multiponto. Velocidades de 64 Kbps a 2 Mbps;
- **DataSat Uni**: Serviço de difusão de mensagem, unidirecional, para estações tipo VSAT (Very Small Aperture Terminal);
- **DataSat Bi**: Serviço bidirecional para estações tipo VSAT. Se as estações terrenas forem da Embratel, chama-se Compartilhado. Se as estações terrenas forem do cliente, chama-se Exclusivo.

Sistemas Por Cabo

Par Trançado: O par trançado foi um sistema originalmente produzido para transmissão telefônica para sinais elétricos analógicos (tal é o caso da voz humana após de uma etapa de transdução). Interessante observar que utilizando o sistema de transmissão por par de fios aproveita-se esta tecnologia que já é tradicional por causa do seu tempo de uso e do grande número de linhas instaladas. A taxa de transmissão varia de acordo com as condições das linhas telefônicas utilizadas, podendo variar entre 9600 a 19200 bps. Considerando enlaces ponto a ponto, essas taxas são bem aceitáveis, porém quando se trata de enlaces multiponto, a taxa de transmissão decresce significativamente.

Todo o meio físico de transmissão sofre influências do meio externo acarretando em perdas de desempenho nas taxas de transmissão. Essas perdas podem ser atenuadas limitando a distância entre os pontos a serem ligados.

A qualidade das linhas de transmissão que utilizam o par de fios depende, basicamente, da qualidade dos condutores empregados, bitola dos fios (quanto maior a bitola, mais corrente passa pelo condutor), técnicas usadas para a transmissão dos dados através da linha e proteção dos componentes da linha para evitar a indução dos condutores.

A indução ocorre devido a alguma interferência elétrica externa ocasionada por osciladores, motores ou geradores elétricos, mau contato ou contato acidental com outras linhas de

transmissão que não estejam isolados corretamente ou até mesmo tempestades elétricas ou proximidades com linhas de alta tensão. A vantagem principal na utilização do par de fios ou par trançado é seu baixo custo de instalação e manutenção, considerando o grande número de bases instaladas.

Cabo Coaxial: Possui vantagens em relação aos outros condutores utilizados tradicionalmente em linhas de transmissão por causa de sua blindagem adicional, que o protege contra o fenômeno da indução, causado por interferências elétricas ou magnéticas externas. Essa blindagem constitui-se de uma malha metálica (condutor externo) que envolve um condutor interno isolado.

Os cabos coaxiais geralmente são empregados na ligação de pontos próximos um do outro (rede local de computadores, por exemplo). A velocidade de transmissão é bastante elevada devido à tolerância aos ruídos graças a malha de proteção desses cabos.

Os cabos coaxiais são divididos em duas famílias:

1. **Banda Base**: Nesta tecnologia de transmissão, o sinal digital é injetado diretamente no cabo. A capacidade de transmissão dos cabos nesta modalidade varia entre alguns Mbps/Km, no caso dos cabos mais finos, até algumas dezenas de Megabits por segundo no caso de cabos grossos. A impedância utilizada nesta modalidade de transmissão é de 50 Ohms.

2. **Banda Larga**: Nesta tecnologia de transmissão, os cabos coaxiais suportam uma banda passante de até 400Mhz. Devido a esta grande tolerância, esse cabo é muito utilizado para a transmissão do sinal de vídeo em TV a cabo e, na transmissão de vídeo também em computadores, para a integração de imagens transmitidas para várias estações de rede local. A impedância utilizada nesta modalidade de transmissão é de 75 Ohms.

As dificuldades de conexão com cabos coaxiais são um pouco maiores do que se fosse utilizado o par trançado. A conexão dos cabos é feita através de conectores mecânicos, o

que também encarece sua instalação em relação ao par trançado, porém, os benefícios compensam com larga vantagem a utilização deste método.

Fibras Ópticas: São elementos de transmissão que utilizam sinais de luz codificados para transmitir os dados. A luz que circula pela fibra óptica situa-se no espectro do infravermelho e seu comprimento de onda está entre 10^{14} a 10^{15} Hz. A fibra óptica pode ser feita de plástico ou de vidro, revestida por um material com baixo índice de refração. Além destes dois materiais, a fibra possui também um revestimento plástico que lhe garante uma proteção mecânica contra o ambiente externo.

Para a transmissão dos sinais, além do cabo precisa-se de um conversor de sinais elétricos para sinais ópticos, um transmissor e um receptor dos sinais ópticos, e um conversor dos sinais ópticos para os sinais elétricos. Nas linhas de fibras ópticas, a taxa de transmissão é muito mais alta do que nos sistemas físicos convencionais (cabo coaxial e par trançado).Isto deve-se ao fato de que a atenuação das transmissões não dependem da frequência utilizada.

A fibra óptica é completamente imune a interferências eletromagnéticas, portanto, não sofre indução, podendo ser instalada em lugares onde os fios e cabos não podem passar. Também não precisa de aterramento e mantém os pontos (que liga eletricamente) isolados um do outro.

Modos De Transmissão

A informação é geralmente transmitida sequencialmente na rede em blocos de tamanho fixo (normalmente múltiplo de 8 bits). Na presença de erros, isto permite que só os blocos corrompidos sejam retransmitidos, reduzindo o tempo de recuperação de erros de transmissão.

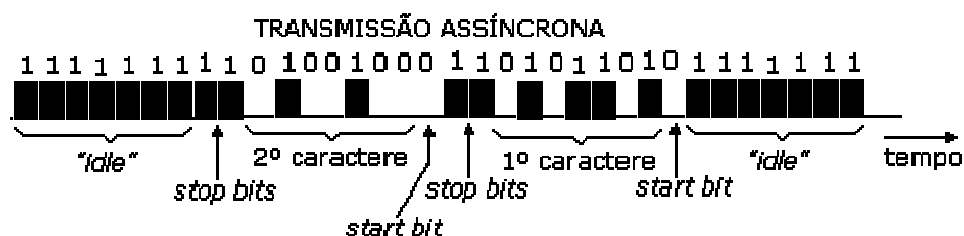
Os dispositivos de rede recebem, então, essa sequência de blocos e tentam reconstruir a informação transmitida. Para que tanto a recepção como a reconstrução da informação seja possível, é necessário que o transmissor e o receptor conheçam certos detalhes tais como,

débito da rede, princípio e fim de um bloco, etc., de tal maneira de permitir a decodificação e interpretação dos conteúdos dos blocos.

A sincronização pode ser conseguida de duas maneiras diferentes. Se a informação é transmitida em intervalos aleatórios, cada dispositivo tem de ser capaz de se resincronizar no início da recepção de cada bloco - transmissão assíncrona. Este modo de transmissão obriga o encapsulamento do bloco em bits de sinalização especiais que indicarão o seu princípio e fim (Start e Stop bits). Pelo contrário, se a informação é transmitida em intervalos de tempo fixos, o transmissor e o receptor podem estar em sincronia por muito tempo, sincronizando-se através de informação especial introduzida nos blocos de dados, este é o caso da transmissão síncrona.

Transmissão Assíncrona

Na transmissão assíncrona, o intervalo de tempo entre os caracteres transmitidos não é fixo. Podemos exemplificar com um digitador operando um terminal, não havendo um fluxo homogêneo de caracteres a serem transmitidos. Como o fluxo de caracteres não é homogêneo, não haveria como distinguir a ausência de bits sendo transmitidos de um eventual fluxo de bits zero e o receptor nunca saberia quando virá o próximo caractere e, portanto, não teria como identificar o que seria o primeiro bit do caractere.

Para resolver esses problemas de transmissão assíncrona, foi padronizado que na ausência de caracteres a serem transmitidos o transmissor mantém a linha sempre no estado 1 (isto é, transmite ininterruptamente bits 1, o que distingue também de linha interrompida).

Quando for transmitir um caractere, para permitir que o receptor reconheça o início do caractere, o transmissor insere um bit de partida (Start bit) antes de cada caractere. Convenciona-se que esse Start bit será um bit zero, interrompendo assim a sequência de bits 1 que caracteriza a linha livre (Idle). Para maior segurança, ao final de cada caractere o transmissor insere um (ou dois dependendo do padrão adotado) bits de parada (Stop bits), convencionando-se a serem bits 1 para diferenciá-los dos bits de partida.

Os bits de informação são transmitidos em intervalos de tempo uniformes entre o Start bit e o(s) Stop bit(s). Portanto, transmissor e receptor somente estarão sincronizados durante o intervalo de tempo entre os bits de Start e Stop. A transmissão assíncrona também é conhecida como "Start-Stop".

A taxa de eficiência de uma transmissão de dados é medida como a relação de número de bits úteis dividido pelo total de bits transmitidos. No método assíncrono, a eficiência é menor que a no método síncrono, uma vez que há necessidade de inserir os bits de partida (Start) e parada (Stop), de forma que a cada caractere são inseridos de 2 a 3 bits que não contém informação. A transmissão assíncrona é utilizada em comunicações de baixa velocidade. Baseado no exposto anteriormente pode-se definir algumas vantagens e desvantagens do modo de transmissão assíncrona.

Vantagens

- Existe resincronização no início de cada caractere transmitido.
- Esquema simples e econômico.

Desvantagens

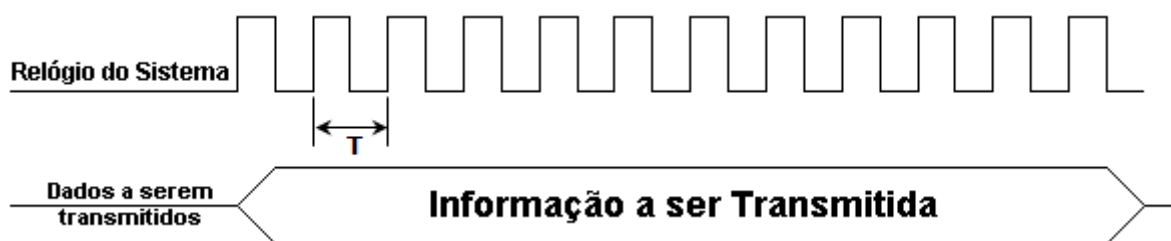
- Apresenta uma carga de processamento (overhead) excessivo (em geral > 20%).
- Apesar de tudo podem ocorrer erros.

- Um exemplo de comunicação assíncrona é quando dois computadores estão conectados via porta serial pela interface EIA RS-232C (V.24).

Transmissão Síncrona

Na forma de transmissão síncrona o processo é mais sofisticado, pois não existem sinais intermitentes de início e fim. Os sinais iniciais são chamados de bytes de sincronização (Sync). O modo de transmissão síncrono é uma maneira de transmitir bits de forma que estes possam ser recebidos adequadamente pelo receptor. No entanto, para que a informação enviada seja corretamente interpretada, o receptor deve conhecer a priori os instantes que separam os bits dentro do caractere.

Neste modo de transmissão, o receptor e o transmissor estão sincronizados quase que permanentemente, pois existe uma relação direta entre tempo e os caracteres transferidos, mesmo assim podem ocorrer perdas de sincronismo durante a transmissão.

O receptor conhecendo os intervalos de tempo representativos dos bits identifica a sequência de bits transmitida, fazendo uma amostragem do sinal recebido em intervalos regulares de T segundos. Essa temporização básica corresponde ao sinal de relógio (Clock de sincronismo) de período T segundos que estabelece a taxa ou velocidade de transmissão 1/T, expressa normalmente em bits por segundo (bps).

O início da transmissão é feito pelo envio de uma configuração de bits chamada caractere de sincronização (ou Sync) antes de a mensagem ser transmitida. O conjunto de caracteres que formam uma mensagem é dividido em blocos.

Para que ocorra a sincronização e esta amostragem possa ser feita nos instantes apropriados (mesma cadência de emissão dos bits), ocorre o envio de uma configuração de bits de sincronização no início do bloco a ser transmitido. Contudo, se o bloco é muito extenso, algumas máquinas costumam ressincronizar seus osciladores, enviando, no interior do bloco, caracteres de sincronização, principalmente em mensagens muito longas. Este caractere deve ser precisamente diferenciado dos demais para não haver ressincronização no momento errado.

Neste sentido são utilizadas técnicas de transparência. Quando o envio é feito antes da formação do bloco, os caracteres são armazenados no buffer do equipamento receptor até que todos estejam completos para a formação do bloco. Quando não há caracteres a serem transferidos, o transmissor continua enviando caracteres especiais de forma que o intervalo de tempo entre caracteres se mantém constante e o receptor mantenha o sincronismo.

Deve-se observar que o modo de transmissão síncrono é mais utilizado quando as máquinas usadas transmitem sua informação continuamente na linha, fazendo assim uma utilização mais eficiente desta. Neste modo, os bits de um caractere são seguidos imediatamente pelos próximos, não havendo delimitadores de caractere (Start/Stop bits) como na transmissão assíncrona.

A montagem desses blocos de transmissão (com tamanho fixo ou variável) exige o uso de Buffers (memória) para acumular as informações e armazená-las antes da transmissão ou na recepção. Portanto, a partir das características apresentadas, podem-se definir algumas vantagens e desvantagens do modo de transmissão síncrono.

Vantagens

- Em relação à transmissão assíncrona, é mais eficiente, pois a proporção de informação para sinais de controle (sincronização) é bem maior, não necessitando de sinais de início e fim de caractere (Start/Stop bits).

- Facilita o uso de algoritmos de compactação devido ao armazenamento em buffer. Isto permite aumentar a velocidade de transmissão.
- A transmissão síncrona oferece melhor proteção contra erros, pois, existe no final deste um conjunto de caracteres para verificação de erros: BCC (Block Check Character).

Desvantagens:

- Se há um erro de sincronização, todo o bloco é perdido, pois até a ressincronização a amostragem será realizada em instantes incorretos.
- Exige o uso de Buffers (memória), o que encarece o custo do equipamento, pois os caracteres devem ser enviados em blocos e não conforme sua disponibilidade.

UNIDADE 5

Objetivo: Saber identificar, pelo tamanho físico, o tipo de rede empregada.

Redes de Computadores (Parte I)

Conceito de Redes

Uma rede de computadores é um conjunto de computadores (locais ou remotos) interligados entre si (de forma total ou parcial) de tal maneira de possibilitar a comunicação de dados localmente e/ou remotamente, incluindo todos os equipamentos eletrônicos necessários à interconexão de dispositivos, tais como microcomputadores e impressoras. Esses dispositivos que se comunicam entre si são chamados de nós, estações de trabalho, pontos ou simplesmente dispositivos de rede. Bastariam só dois computadores, ou nós, como o número mínimo de dispositivos necessários para formarmos uma rede. O número máximo não é predeterminado, pois, teoricamente, todos os computadores do mundo poderiam estar interligados, de fato a Internet é um exemplo disto.

Uso das Redes (Comercial e Doméstico)

As principais finalidades do uso das redes nas organizações são:

- A economia e compartilhamento de recursos
- A confiabilidade das informações

Pois tendo os equipamentos conectados, os sistemas são compartilhados, tornando-os acessíveis para todos os usuários, evitando assim informações duplicadas ou desatualizadas.

As redes de computadores estão diretamente relacionadas com a confiabilidade do sistema. A continuidade de funcionamento de um sistema é primordial para as aplicações, como por exemplo: aplicações de tráfego aéreo, transações bancárias, comunicações militares, etc.

De uma forma geral o objetivo de uma rede de computadores é tornar disponível a qualquer usuário todos os programas, dados e outros recursos independentes de sua localização física, proporcionando uma maior disponibilidade e confiabilidade, dada a possibilidade de migração para outro equipamento quando a máquina sofrer alguma falha. Desta forma, as redes de computadores viabilizam um meio de comunicação poderoso, devido a sua velocidade, confiabilidade e compartilhamento dos recursos.

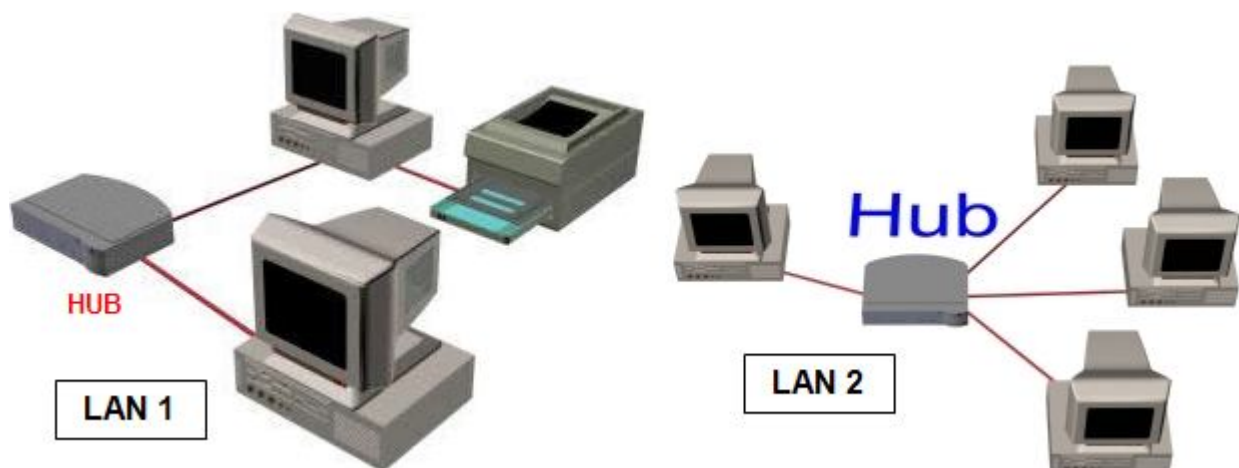
Foi por esses motivos que as organizações reconheceram o quanto poderiam economizar e ganhar em produtividade usando as redes. Começou-se então a implantá-las e a expandir as já existentes, e rapidamente surgiram novos produtos e novas tecnologias para as mesmas.

Classificação das Redes (LAN, MAN e WAN)

No início dos anos 80 houve uma grande expansão no campo das redes, mas logo foram sentidos os problemas desse crescimento acelerado. Muitas das tecnologias de rede criadas eram baseadas em diferentes plataformas de hardware e software que não eram compatíveis, o que dificultou a comunicação entre si, ou seja, o objetivo principal de compartilhar informação e recursos entre redes não era atingido. Foi então que as redes foram divididas e a troca de informações passou a variar conforme a classificação dada a seguir.

Redes de Área Local, LAN (Local Area Networks)

A rede de área local é a responsável pela comunicação entre computadores em uma área restrita, compartilhando recursos de hardware, software e informações.

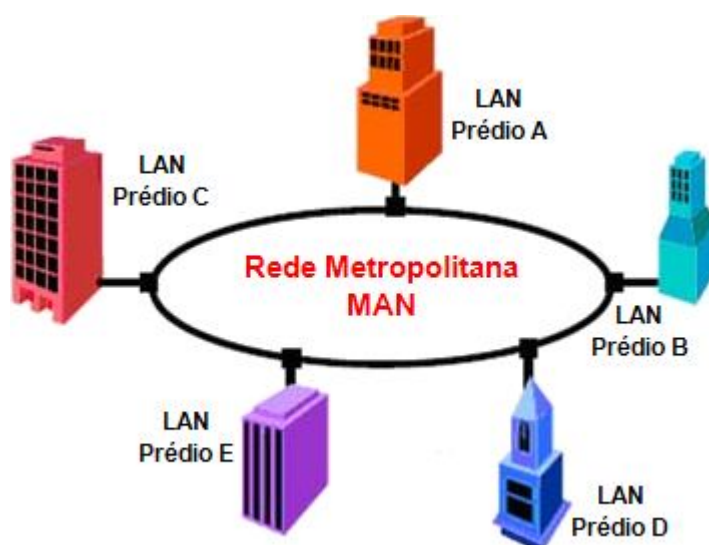
As redes locais são encontradas em escritórios, empresas, universidades e na maioria das organizações onde a comunicação entre diferentes departamentos e compartilhamento de recursos é necessária. Nas LANs tradicionais os computadores são conectados por cabos ou através de equipamentos chamados HUBS, como exemplo, a figura abaixo apresenta duas redes LAN independentes. Neste tipo de rede a velocidade de transmissão geralmente varia de 10 a 100 Mbps, havendo um retardo muito baixo (quase desprezível) e os erros de transmissão encontrados são pouquíssimos.

Entretanto as atuais redes LANs podem operar ainda com velocidades mais altas, por exemplo, as redes FastEthernet, GigaEthernet, 10GigaEthernet, etc.

Redes de Área Metropolitana, MAN (Metropolitan Area Networks)

As redes metropolitanas são redes de dimensão média, ocupam aproximadamente o espaço de uma cidade, constituída de uma ou mais redes LANs. Portanto, uma MAN pode abranger um grupo de escritórios vizinhos ou uma cidade inteira e pode ser privada ou pública. Conforme mostra a figura, uma rede metropolitana é uma versão ampliada de uma LAN, pois utilizam tecnologias semelhantes.

Este tipo de rede pode transportar voz e dados podendo inclusive ser associado à rede de televisão a cabo local. As MANs são comuns em universidades hospitais e em organizações com várias delegações espalhadas ao longo de espaço metropolitano.

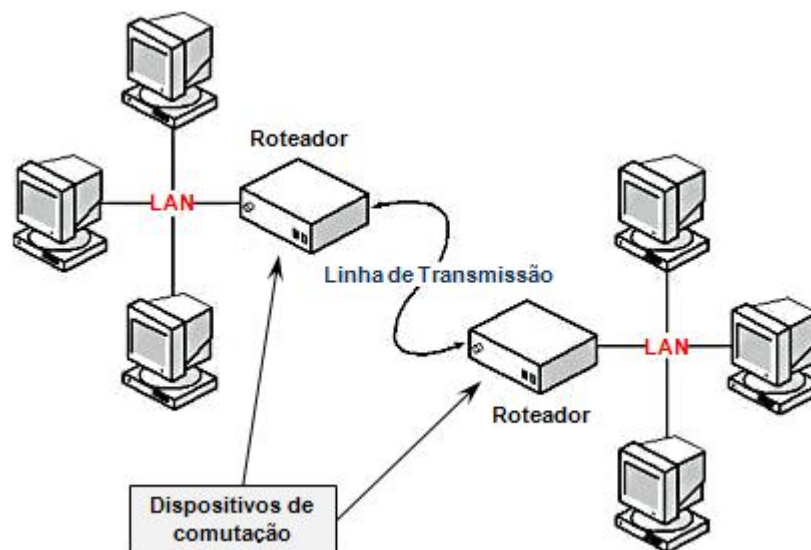
As características mais importantes de uma MAN são:

- Interligação de LANs com uma distância que cubra uma cidade ou campus;
- Utilizam tecnologias semelhantes das LANs (Ethernet, Token Ring, etc.);
- Apresentam uma taxa de erro um pouco maior se comparada com as redes LANs por causa do tamanho;
- Otimizam a relação custo/benefício devido à utilização de tecnologias semelhantes às das LANs.

Redes de Área Geograficamente Estendida, WAN (Wide Area Networks)

A história das redes WAN começa em 1965 quando Lawrence Roberts e Thomas Merril ligaram dois computadores, um TX-2 em Massachussets a um Q-32 na Califórnia, através de uma linha telefônica de baixa velocidade, criando a primeira rede de área estendida (WAN).

A maior WAN que existe atualmente é a própria Internet. Em geral, as redes geograficamente distribuídas contêm conjuntos de servidores, que formam grandes e variadas sub-redes.

Essas sub-redes têm a função de transportar os dados entre os computadores ou dispositivos de rede. Atualmente as redes WAN se tornaram extremamente necessárias devido ao crescimento das corporações, onde as LAN não eram mais suficientes para atender a demanda de informações compartilhadas, pois era necessária uma forma de passar informação de uma empresa para outra de forma rápida e eficiente. Surgiram as WAN que conectam redes dentro de uma vasta área geográfica, permitindo comunicação de longa distância.

As WAN abrangem amplas áreas geográficas, com cobertura em nível nacional ou mesmo internacional. As WANs contém um conjunto de computadores cuja finalidade é executar aplicações que estão conectados por várias sub-redes de comunicação transportando mensagens de um ponto geográfico para outro.

Na maioria das WANs, conforme mostra a figura, a sub-rede consiste em dois componentes distintos: linhas de transmissão e dispositivos de comutação. As linhas de transmissão, também chamadas de circuitos, canais ou troncos, transportam os bits entre os computadores. Os dispositivos de comutação são equipamentos especializados usados para

conectar duas ou mais linhas de transmissão, no caso de uma rede WAN os dispositivos de comutação são denominados: Roteadores (ou Routers, em inglês).

Em síntese uma rede WAN é uma rede de comunicação de dados que cobre uma área geográfica relativamente extensa e que oferece uma transmissão (de dados) provida por operadoras, como empresas de telefonia e telecomunicações. As tecnologias WAN geralmente funcionam nas três primeiras camadas do modelo OSI, a saber:

1. **Camada Física**: X.21, EIA/TIA 232, EIA/TIA-449, V.24, V.35, HSSI, G.703, EIA-530.
2. **Camada de Enlace de Dados (Data Link)**: NLACE - LAPB, Frame-Relay, HDLC, PPP, SDLC.
3. **Camada de Rede**: X.25, PLP, IP.

Em função dos custos de comunicação serem bastantes altos, em geral estas redes são públicas. Um exemplo claro de uma rede WAN é a própria Internet que conecta milhões de redes LAN no mundo todo formando uma WAN (lembrar que Internet = Inter + Networks, ou seja, trabalho entre redes).

Na maioria das WANs, a rede contém numerosos cabos ou linhas telefônicas, todos conectados a um par de roteadores. No entanto, se dois roteadores que não compartilham um cabo desejarem se comunicar, eles só poderão fazê-lo através de outros roteadores. Quando os pacotes de informação são enviados de um roteador local para outro roteador de destino é bem possível que esses pacotes atravessem um caminho que poderia consistir de um ou mais roteadores intermediários, cada pacote é recebido integralmente em cada roteador do caminho, onde é armazenado até a linha de saída solicitada ser liberada, para então ser encaminhado.

As sub-redes que utilizam esse princípio são chamadas de sub-redes do tipo ponto-a-ponto, Store-and-Forward ou de comutação por pacotes. Quase todas as redes de área estendida ou geograficamente distribuída (com a exceção das que utilizam satélites) têm sub-redes do

tipo Store-and-Forward, basicamente estas redes, realizam a tarefa de armazenar temporariamente as mensagens recebidas, em buffers (memórias) internas e uma vez completas essas mensagens são encaminhadas para o seguinte salto e assim sucessivamente até chegar ao destino final, daí o nome de armazenar e encaminhar (Store-and-Forward).

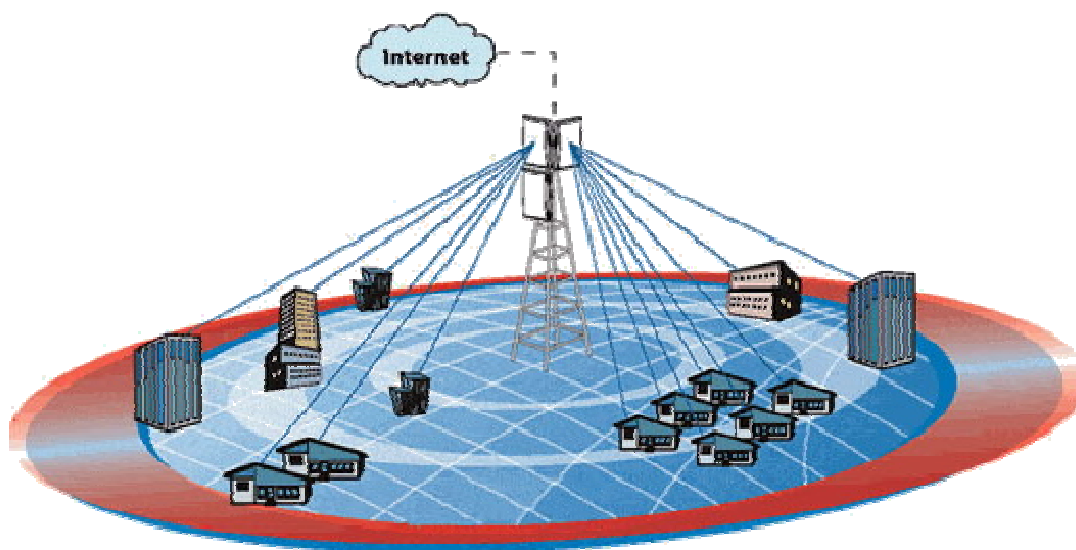
UNIDADE 6

Objetivo: Entender o funcionamento das redes sem-fio (Wireless).

Redes de Computadores (Parte II)

Redes Sem Fio ou Wireless

As redes Wireless (redes sem-fio) constituem um segmento de mercado que vem crescendo muito nos últimos anos. Este tipo de redes são soluções normalmente aplicadas onde uma infraestrutura de cabeamento convencional (cobre ou fibra óptica) não pode ser utilizada. Estas redes são muito utilizadas por empresas.

A sua principal vantagem é fato de dispensar os fios e a mobilidade, sendo o ideal para ambientes onde a passagem de cabos é inviável. Embora, este tipo de redes tinha inicialmente sua velocidade de transmissão extremamente baixa, atualmente este tópico foi melhorado bastante pelos que desenvolvem da tecnologia Wireless e temos taxas de transmissão elevadas para este tipo de redes.

Redes Wireless viabilizam dessa forma o atendimento de pontos de rede com a mesma eficiência e até mesmo uma melhor relação custo/benefício em relação ao sistema de cabeamento convencional nesses casos.

Embora ainda persistam algumas dúvidas e discussões sobre a confiabilidade e eficiência das redes sem-fio no que diz respeito à segurança na transmissão da informação, existe um consenso sobre sua fácil configuração, eficiente controle e gerenciamento de dispositivos e simplicidade para alterações do layout.

A instalação de redes Wireless (e vários pontos de acesso à rede) elimina a necessidade de se instalar novos cabos, reduzindo o tempo de configuração de novas posições de trabalho e facilitam a construção de estruturas provisórias como quiosques, salas de treinamento, etc. Uma rede Wireless proporciona, dessa forma, todas as funcionalidades de uma rede com cabos, porém sem as restrições físicas do cabeamento propriamente dito.

Classificação Das Redes Sem Fios

A sequência da abrangência de cobertura das tecnologias sem-fio é a seguinte: WPAN (Wireless Personal Área Network), WLAN (Wireless Area Network), WWAN (Wireless Wide Area Netwotk) - empresas convencionais de telefonia móvel e WMAN (Wireless Metropolitan Area Network)

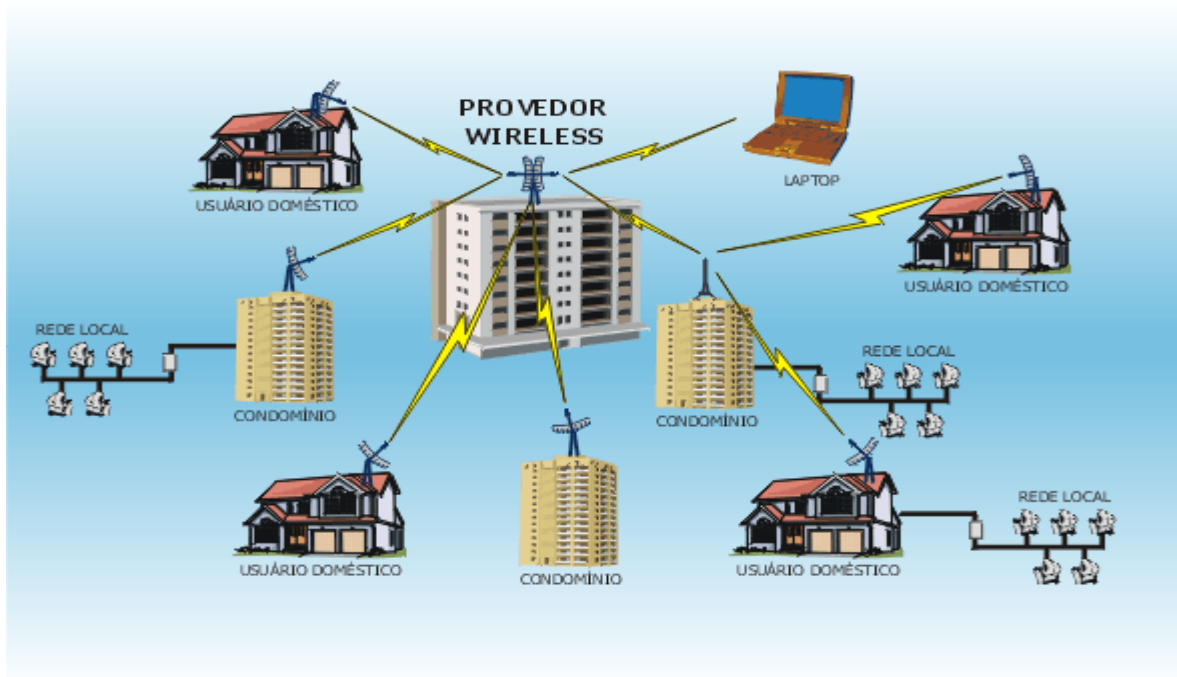
- **Wireless Personal Area Network (WPAN)**: Como o nome indica é uma rede local pessoal sem-fio. Normalmente utilizada para interligar dispositivos eletrônicos fisicamente próximos, os quais não se querem que sejam detectados à distância. Este tipo de rede é ideal para eliminar os cabos usualmente utilizados para interligar teclados, impressoras, telefones móveis, agendas eletrônicas, computadores de mão, câmaras fotográficas digitais, mouses e outros. Nos equipamentos mais recentes é utilizado o padrão Bluetooth para estabelecer esta comunicação, mas também é empregado raio infravermelho (semelhante ao utilizado nos controles remotos de televisores). Detalhes no tópico Bluetooth.

- **Wireless Local Area Network (WLAN)**: A rede WLAN é uma rede local que usa ondas de rádio para fazer uma conexão Internet, ao contrário da rede fixa ADSL ou conexão-TV, que geralmente usa cabos. WLAN já é muito importante como opção de conexão em muitas áreas de negócio. Inicialmente as WLANs inicialmente foram instaladas nas universidades, nos aeroportos, e em outros lugares públicos principais. A diminuição dos custos do equipamento de WLAN fez com que estas redes cheguem a lugares particulares.

  Entretanto, no Reino Unido o custo de usar tais conexões limitou-se o uso aos lounges das Businessclass dos aeroportos. Nova Iorque começou mesmo um programa piloto para cobrir todos os quarteirões do centro da cidade com a Internet Wireless com planejamento de expansão para os bairros suburbanos. Originalmente a WLAN era muito cara e foi somente usada como uma alternativa ao LAN-Internet com cabo nos lugares onde instalar cabos era difícil ou impossível. Tais lugares poderiam ser edifícios ou salas de aula velhas, embora a escala restrita o padrão IEEE 802. 11b limite seu uso aos edifícios menores. Os componentes de WLAN são agora baratos o bastante para ser usado nas horas de repouso e podem ser utilizados para compartilhar uma conexão Internet com a família inteira.

  Desenvolvimentos foram feitos nos padrões de transmissão com os protocolos proprietários, mas no fim dos anos 90 estes foram substituídos por padrões, de várias versões IEEE 802.11 (Wi-Fi) ou HomeRF (2 Mb/s), para o uso caseiro. A falta da segurança das conexões Wireless é um ponto fraco, porém muitas (ADSL) conexões Broadband são oferecidas agora junto com um ponto de acesso Wireless com possibilidade de usar protocolos mais seguros como o WPA. Muitas máquinas Laptops

já vêm com o Networking Wireless Centrino instalado e assim elimina a necessidade de um cartão adicional do encaixe (PCMCIA). O uso de WindowsXP como 'padrão' torna muito fácil configurar um PC como cliente de WLAN e permite aos PCs o acesso a Internet através dos Hotspots (estações base). Entretanto, a falta da perícia em ajustar tais sistemas significa frequentemente que seu vizinho poderia compartilhar também de sua conexão Internet, às vezes sem você (ou eles) se darem conta. A frequência em que 802.11b opera é de 2.4GHz, esta freqüência de operação pode conduzir a interferências com muitos telefones sem fio.

- **Wireless Wide Area Network (WWAN)**: Basicamente o conceito de uma rede WWAN chega a ser o mesmo dado a uma rede WAN, portanto, uma WWAN constitui o conjunto (é o agregado, a soma) de redes WMAN e WLAN que estão geograficamente distribuídas. Na prática não é comum ouvir se falar de WWAN, mas sim somente de WLAN e WMAN.

- **Wireless Metropolitan Area Network (WMAN)**: Este tipo de redes tem bastante visibilidade atualmente por ser uma alternativa à tecnologia de telefonia móvel vigente

- temos os padrões IEEE 802.16 e IEEE 802.20. Para conhecer um pouco sobre WMAN veja as referências: 802.16: *A Future Option for Wireless MANs do 802.11 Planet, Wireless to the max - WiMAX* do site Arcchart.

Padrões E Tecnologias

Entre os vários padrões e tecnologias dentro das redes Wireless podem-se mencionar as seguintes:

- IrDA - Infrared Data Association.
- ZigBee (IEEE 802.15.4).
- Bluetooth (IEEE 802.15.1): É uma tecnologia para a comunicação sem-fio entre dispositivos eletrônicos a curtas distâncias (ambiente WLAN).
- RONJA é uma tecnologia livre e aberta para a comunicação sem-fio Ponto-a-Ponto (P2P) por meio de luz do espectro visível ou infravermelho através do ar.
- Wi-Fi (IEEE 802.11): Basicamente é uma tecnologia desenvolvida para WLAN.
- WiMAX (IEEE 802.16): Tecnologia desenvolvida para WWAN.
- Mesh (IEEE 802.11s).

De todos esses padrões e tecnologias mencionadas acima serão dados a seguir uma visão geral das mais relevantes na atualidade.

Bluetooth (IEEE 802.15.1)

O Bluetooth é um padrão para redes PAN (Personal Area Network), ou seja, uma rede de curta distância, portanto, esta tecnologia permite uma comunicação simples, rápida, segura e

de baixo custo entre computadores, smartphones, telefones celulares, mouses, teclados, fones de ouvido, impressoras e outros dispositivos, utilizando ondas de rádio no lugar de cabos. Assim, é possível fazer com que dois ou mais dispositivos comecem a trocar informações com uma simples aproximação entre eles.

Bluetooth é um padrão global de comunicação sem-fio e de baixo consumo de energia que permite a transmissão de dados entre dispositivos compatíveis com a tecnologia. Para isso, uma combinação de hardware e software é utilizada para permitir que essa comunicação ocorra entre os mais diferentes tipos de aparelhos. A transmissão de dados é feita através de radiofrequência, permitindo que um dispositivo detecte o outro independente de suas posições, desde que estejam dentro do limite de proximidade.

Para que seja possível atender aos mais variados tipos de dispositivos, o alcance máximo do Bluetooth foi dividido em três classes, a saber:

1. **Classe 1**: potência máxima de 100 mW com alcance de até 100 metros;
2. **Classe 2**: potência máxima de 2,5 mW com alcance de até 10 metros;
3. **Classe 3**: potência máxima de 1 mW com alcance de até 1 metro.

Isso significa que um aparelho com Bluetooth Classe 3 só conseguirá se comunicar com outro se a distância entre ambos for inferior a 1 metro, por exemplo. Neste caso, a distância pode parecer inutilizável, mas é suficiente para conectar um fone de ouvido a um telefone celular pendurado na cintura de uma pessoa. É importante frisar, no entanto, que dispositivos de classes diferentes podem se comunicar sem qualquer problema, bastando respeitar o limite daquele que possui um alcance menor.

Deve-se ressaltar que, na maioria dos casos, o alcance efetivo dos dispositivos de Classe 2 é estendido se eles se conectam a dispositivos de Classe 1, se comparados com redes puras de Classe 2. Isso pode ser obtido pela alta sensibilidade e potência de transmissão do dispositivo de Classe 1. A alta potência de transmissão do dispositivo de Classe 1 permite a

recepção da alta potência pelo dispositivo de Classe 2. Além disso, a alta sensibilidade do dispositivo de Classe 1 permite a recepção da baixa potência de transmissão de força dos dispositivos de Classe 2, permitindo assim a operação de dispositivos de Classe 2 a grandes distâncias.

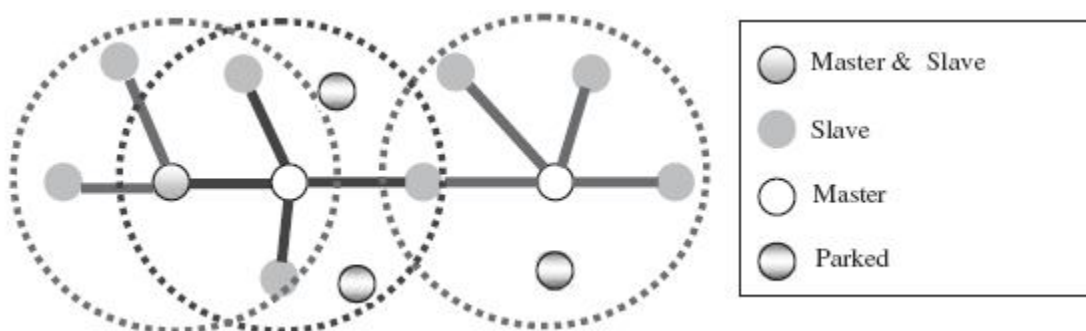
Dispositivos que possuem um amplificador de potência na transmissão têm uma sensibilidade de recepção melhorada, e existem antenas altamente otimizadas que normalmente alcançam distâncias de 1 km usando o padrão Bluetooth Classe 1.

A velocidade de transmissão de dados no Bluetooth é baixa: até a versão 1.2, a taxa pode alcançar, no máximo, 1 Mbps. Na versão 2.0, esse valor passou para até 3 Mbps. Embora essas taxas sejam curtas, são suficientes para uma conexão satisfatória entre a maioria dos dispositivos.

O Bluetooth é uma tecnologia criada para funcionar no mundo todo, razão pela qual se fez necessária a adoção de uma frequência de rádio aberta, que seja padrão em qualquer lugar do planeta. A faixa ISM (Industrial, Scientific, Medical), que opera à frequência de 2,45 GHz, é a que me mais se aproxima dessa necessidade e é utilizada em vários países, com variações que vão de 2,4 GHz à 2,5 GHz. Um dispositivo utilizando Bluetooth pode tanto receber quanto transmitir dados em modo Full-Duplex.

Quando dois ou mais dispositivos se comunicam através de uma conexão Bluetooth, eles formam uma rede denominada piconet. Nessa comunicação, o dispositivo que iniciou a conexão assume o papel de Master (mestre), enquanto que os demais dispositivos se tornam Slaves (escravos). Cabe ao Master a tarefa de regular a transmissão de dados entre a rede e o sincronismo entre os dispositivos.

Cada piconet pode suportar até 8 dispositivos (um Master e 7 Slaves), no entanto, é possível fazer com esse número seja maior através da sobreposição de piconets. Em poucas palavras, isso significa fazer com que uma piconet se comunique com outra dentro de um limite de alcance, este esquema é denominado de Scatternet.

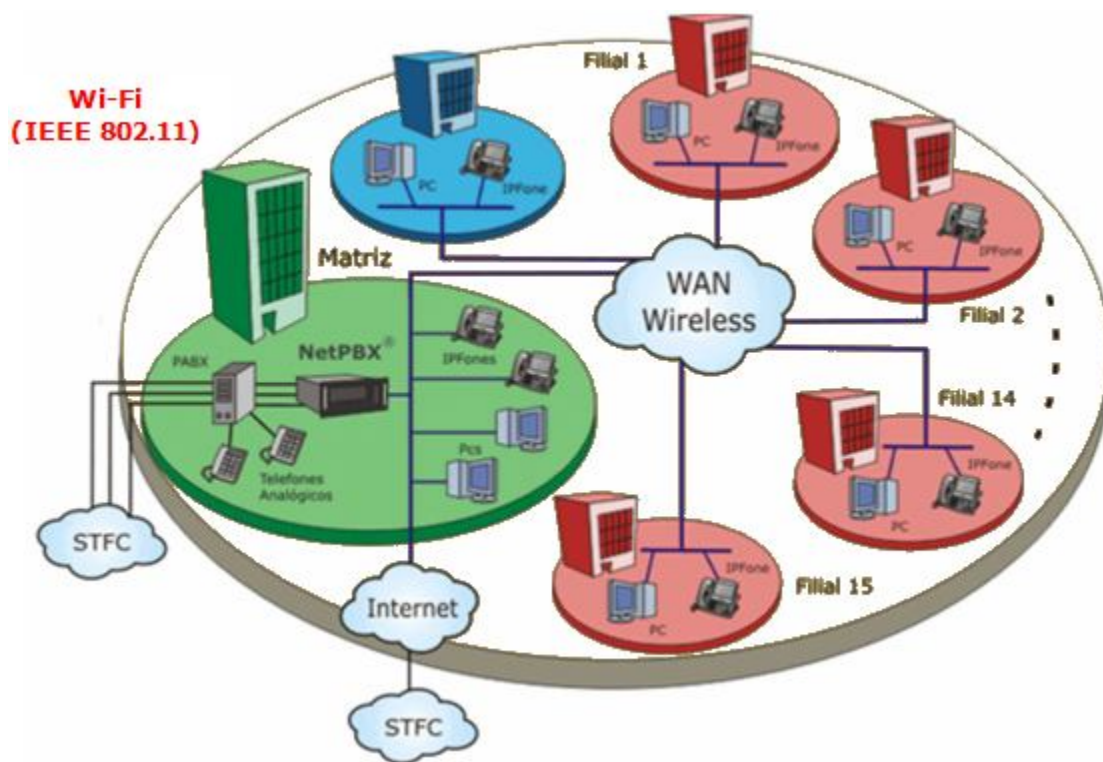
Na figura apresenta-se um exemplo de uma rede Bluetooth com 3 piconets, 3 Masters, 1 Master/Slave, 8 Slaves ativos e 3 Slaves inativos (Parked). As linhas pontilhadas mostram as coberturas de transmissão de cada Piconet. Deve-se frisar que um dispositivo Slave pode fazer parte de mais de uma Piconet ao mesmo tempo, no entanto, um Master só pode ocupar essa posição em uma única Piconet.

A versão 2.1 foi lançada em agosto de 2007, tem como principais destaques o acréscimo de mais informações nos sinais Inquiry (permitindo uma seleção melhorada dos dispositivos antes de estabelecer uma conexão), melhorias nos procedimentos de segurança (inclusive nos recursos de criptografia) e melhor gerenciamento do consumo de energia. Para a seguinte versão 3.0 se prevê uma taxa de transferência de 53 a 480 Mbps.

A versão inicial do padrão foi desenvolvida por um consórcio composto pela Ericsson, IBM, Nokia, Toshiba e Intel e publicada em julho de 1999. Pouco depois, o Bluetooth foi adotado pelo IEEE, dando origem ao padrão 802.15.1. Isso reforçou a posição do Bluetooth como um padrão aberto e acelerou sua adoção, embora ele tenha sido ofuscado pelo crescimento do Wi-Fi, que ocupou muitos dos nichos aos quais o Bluetooth era destinado.

O fato de haver várias versões não significa que um dispositivo com uma versão atual não funcione com outro com uma versão inferior, embora possam haver exceções. Todavia, se um dispositivo 2.0 for conectado a outro de versão 1.2, por exemplo, a velocidade da transmissão de dados será limitada à taxa suportada por este último.

Wi-Fi (IEEE 802.11)

Com a popularização das redes Wi-Fi, o mercado ficou com dúvidas em relação ao futuro do Bluetooth, mas os dispositivos com tecnologia Bluetooth ainda se encontram em alta. O Wi-Fi, por sua vez, se mostra mais como um concorrente das tradicionais redes de computadores com fio (padrão Ethernet, em sua maioria). Com a utilização da tecnologia Wireless (Wi-Fi), soluções Wireless antigamente proibitivas ou inviáveis tecnologicamente tornam-se realidade.

Wi-Fi foi uma marca licenciada originalmente pela Wi-Fi Alliance para descrever a tecnologia de redes sem-fios embarcadas (WLAN) baseadas no padrão IEEE 802.11. O termo Wi-Fi foi escolhido como uma brincadeira com o termo "Hi-Fi" e pensa-se geralmente que é uma abreviatura para *Wireless Fidelity*, no entanto a Wi-Fi Alliance não reconhece isso. Comumente o termo Wi-Fi é entendido como uma tecnologia de interconexão entre dispositivos sem-fios, usando o protocolo IEEE 802.11.

O padrão Wi-Fi opera em faixas de frequências que não necessitam de licença para instalação e/ou operação, característica muito interessante e atrativa. No entanto, para uso comercial no Brasil é necessária licença da Agência Nacional de Telecomunicações (Anatel).

Para ter acesso à Internet através de uma rede Wi-Fi é necessário estar dentro do raio de ação ou área de abrangência de um ponto de acesso (normalmente conhecido como Hotspot), ou estar em um local público onde opere uma rede sem-fios. Nestes locais é possível usar dispositivos móveis, tais como, computador portátil, Tablet PC ou PDAs (Assistente Pessoal Digital) com capacidade de comunicação sem-fio, deixando o usuário do Wi-Fi bem à vontade em usá-lo em lugares de "não acesso" à Internet, como: Aeroportos.

Hoje em dia, muitas operadoras de telefonia estão investindo pesado no Wi-Fi, para ganhos empresariais. Os Hotspot Wi-Fi existem para estabelecer os pontos de acesso para conexão à Internet. O ponto de acesso transmite o sinal sem-fios numa pequena distância – cerca de 100 metros. Quando um periférico que permite "Wi-Fi", como um Pocket PC, encontra um Hotspot, o periférico pode na mesma hora conectar-se à rede sem-fio. Como explicado, muitos Hotspots estão localizados em lugares que são acessíveis ao público, como aeroportos, cafés, hotéis e livrarias. Muitas casas e escritórios também têm redes "Wi-Fi". Enquanto alguns Hotspots são gratuitos, a maioria das redes públicas é suportada por Provedores de Serviços de Internet (Internet Service Provider - ISPs) que cobram uma taxa dos usuários para se conectarem. Atualmente praticamente todos os computadores portáteis vêm de fábrica com dispositivos para rede sem-fio no padrão Wi-Fi (802.11b, a ou g). O que antes era acessório está se tornando item obrigatório, principalmente devido ao fato da redução do custo de fabricação.

Os principais padrões na família IEEE 802.11 são:

- **IEEE 802.11a**: Padrão Wi-Fi para frequência 5 GHz com capacidade teórica de 54 Mbps.
- **IEEE 802.11b**: Padrão Wi-Fi para frequência 2,4 GHz com capacidade teórica de 11 Mbps. Este padrão utiliza DSSS (Direct Sequency Spread Spectrum – Sequência Direta de Espalhamento Espectral) para diminuição de interferência.

- **IEEE 802.11g**: Padrão Wi-Fi para frequência 2,4 GHz com capacidade teórica de 54 Mbps.

Na verdade aqui só foram mencionados alguns dos principais padrões da tecnologia Wireless IEEE 802.11, atualmente existem os padrões desde o 802.11a até o padrão IEEE 802.11w. Inclusive temos o padrão 802.11G+ Turbo mode, trabalhando na banda de 2.4 GHz, atingindo uma velocidade de transferência de até os 108 Mbps. Essa característica é proporcionada pelo uso do Chipset (conjunto de circuitos integrados) Atheros.

Temos também o Wi-Fi Protected Access (WPA e WPA2), que é o padrão de segurança desenvolvido para substituir o padrão WEP (Wired Equivalent Privacy) que possui falhas graves de segurança, possibilitando que um hacker (com os meios necessários) pudesse quebrar a chave de criptografia após monitorar poucos minutos de comunicação.

WiMAX (IEEE 802.16)

A tecnologia WiMAX (Worldwide Interoperability for Microwave Access) é um padrão para BWA (Broadband Wireless Access), ou seja, é um acesso sem fio de banda larga para ser utilizado na última milha. O WiMAX atualmente trabalha com os padrões IEEE 802.16d e IEEE 802.16e. O 802.16d (ratificado em Junho de 2004, vide IEEE Scores 802.16d) é o padrão de Acesso Sem-Fio de Banda Larga Fixa (WiMAX Fixo) e cujos equipamentos fizeram os testes de aderência ao padrão e de inter-operabilidade no segundo semestre de 2004 e ficaram disponíveis comercialmente no primeiro semestre de 2005.

O 802.16e (ratificado no final de 2004) é o padrão de Acesso Sem-Fio de Banda Larga Móvel - WiMAX Móvel (assegurando conectividade em velocidades de até 100 Km/h) e cujos equipamentos começaram a ser disponibilizados em 2006. O padrão 802.16d opera em faixa de frequências de 2 a 11 GHz e o 802.16e de 2 a 6 GHz.

O padrão 802.16d é uma evolução do padrão anterior 802.16a homologado em Janeiro de 2003 e já permite um menor consumo de energia e menores CPEs (Customer Premises Equipment) como também inova na incorporação do conceito de Antena MIMO (Multiple Input and Multiple Output).

O WiMAX suporta topologias ponto-multiponto e malha (Mesh). Um lado também bastante inovador nesta tecnologia é que ela opera em bandas de frequências não licenciadas (2,4 e 5,8 GHZ) e em bandas licenciadas (3,5 e 10,5 GHZ). Existe um movimento da FCC americana de buscar mais espectro de frequência a partir da reengenharia de espectro na banda da tecnologia MMDS/ITFS em 2,5 GHz buscando espaço de frequência para novos serviços incluindo o WiMAX.

Este movimento poderia ser seguido no Brasil pela Anatel. A modulação OFDM utilizada no WiMAX pode ser utilizada para proporcionar a conexão "sem linha de visada" (NLOS = Non-

Line of Sight) entre Estações Base e equipamentos de clientes. WiMAX pode atingir um alcance de até 50 Kms, com taxas de dados compartilhadas aproximando-se de 75 Mbps em canalização de 20 MHz.

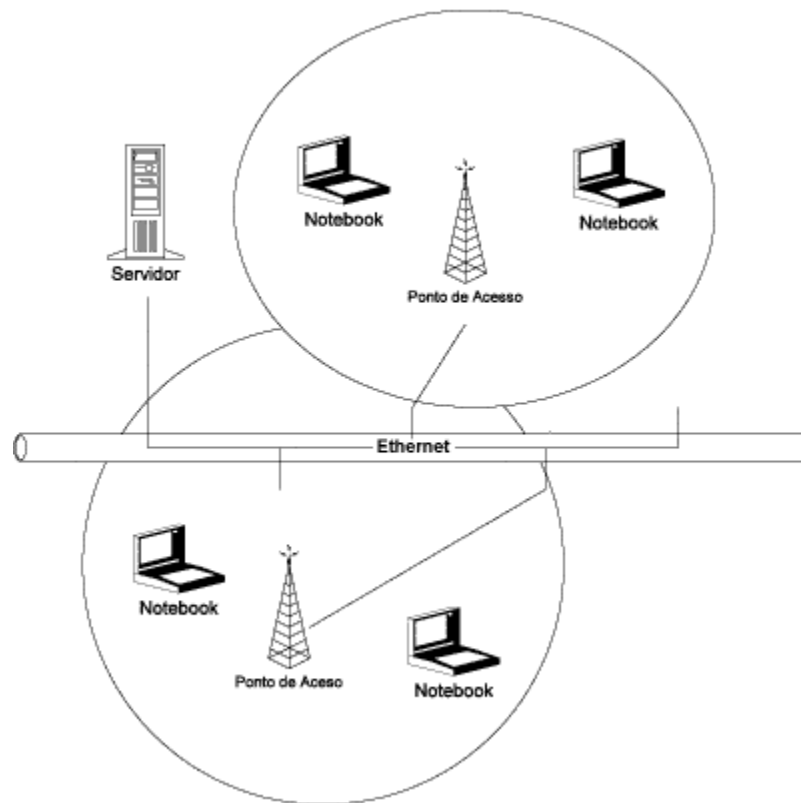
A performance NLOS é assegurada mais fortemente quando se está mais próximo da Estação Base. No alcance máximo de 50 Km espera-se apenas uma performance LOS (Line of Sight). Um raio típico de BWA em NLOS varia de 5 a 8 Km.

Como dito inicialmente, o WiMAX é uma solução de BWA completa para voz, dados e vídeo (Streaming) com QoS (Quality of Service) e Segurança intrínsecas. A Segurança do WiMAX suporta a autenticação com certificados X.509 e criptografia de dados utilizando DES (Data Encryption Standard). O WiMAX pode transportar IPv4, IPv6, Ethernet ou ambos simultaneamente com QoS. Praticamente com o desenvolvimento da tecnologia WiMAX no mercado Wireless, a tecnologia 4G da telefonia celular (do mundo globalizado das comunicações sem-fio) está fazendo seu ingresso.

Funcionamento Básico Das Redes Wireless

Através da utilização portadoras de rádio ou infravermelho, as WLANs estabelecem a comunicação de dados entre os pontos da rede. Os dados são modulados na portadora de rádio e transmitidos através de ondas eletromagnéticas.

Múltiplas portadoras de rádio podem coexistir num mesmo meio, sem que uma interfira na outra. Para extrair os dados, o receptor sintoniza numa frequência específica e rejeita as outras portadoras de frequências diferentes.

Num ambiente típico, o dispositivo transceptor (transmissor/receptor) ou ponto de acesso (access point) é conectado a uma rede local Ethernet convencional (com fio). Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também intermediam o tráfego com os pontos de acesso vizinhos, num esquema de microcélulas com roaming semelhante a um sistema de telefonia celular.

Basicamente a topologia da rede é composta dos seguintes elementos:

- **BSS (Basic Service Set)**: Corresponde a uma célula de comunicação da rede sem-fio.
- **STA (Stations)**: Em uma rede WLAN o termo STA refere-se às estações espalhadas na rede, em outras palavras são os diversos clientes da rede.
- **AP (Access point)**: É o nó que coordena a comunicação entre as STAs dentro da BSS. Funciona como uma ponte de comunicação entre a rede sem-fio e a rede convencional.
- **DS (Distribution System)**: Corresponde ao backbone da WLAN, realizando a comunicação entre os APs.
- **ESS (Extended Service Set)**: Conjunto de células BSS cujos APs estão conectados a uma mesma rede convencional. Nestas condições uma STA pode se movimentar de

uma célula BSS para outra permanecendo conectada à rede. Este processo é denominado de Roaming (função que permite o deslocamento com um sistema de comunicação móvel pela área de cobertura de um outro domínio, por exemplo, um ESS, e se conectar permanentemente ou temporariamente à infraestrutura).

As Redes WLAN podem ser configuradas nos seguintes dois modos:

1. **Modo Ad-hoc (Independent Basic Service Set)**: É o conjunto de serviços básicos de comunicações não infraestruturado (independente). Neste modo de configuração, a comunicação entre as estações de trabalho da WLAN é estabelecida de forma direta, sem a necessidade de um ponto de acesso nem de uma rede física para conectar as estações, ou seja, não se tem uma infraestrutura fisicamente visível. O termo Ad-hoc refere-se justamente à característica não estruturada da rede.

2. **Modo Infraestruturado (Infrastructure Basic Service Set)**: É o conjunto de serviços básicos de comunicações infraestruturado. Neste modo a rede WLAN possui pontos de acessos fixos que permitem a conexão da rede sem-fio à rede convencional e estabelecem a comunicação entre os diversos clientes.

UNIDADE 7

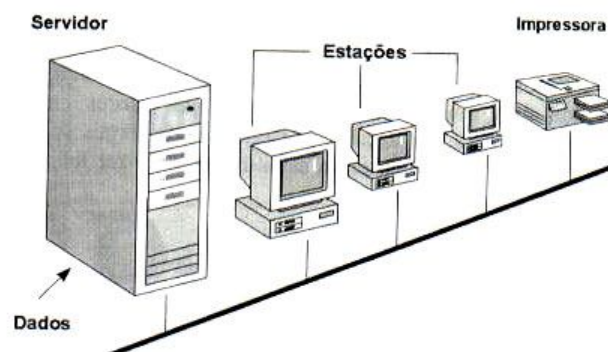
Objetivo: Visualizar e Entender Bem os Conceitos de Redes Cliente/Servidor e P2P.

Redes de Computadores (Parte III)

Redes Cliente/Servidor

É uma arquitetura de rede, onde existem dois módulos básicos na rede: o Servidor e os Clientes. O Servidor é alguma máquina da rede que é responsável por servir os Clientes da rede com aquilo que é solicitado. Clientes são as máquinas que solicitaram informações que estarão contidas no Servidor, ou seja, o processamento da informação é dividido em módulos ou processos distintos. Um processo é responsável pela manutenção da informação (servidores) e outros responsáveis pela obtenção dos dados (os clientes)

É no servidor que normalmente ficam os sistemas mais pesados da rede, tais como o banco de dados. As máquinas clientes são menos poderosas, pois não rodam aplicativos que requerem tantos recursos das máquinas.

O importante em uma máquina em arquitetura Cliente/Servidor não é que todas as máquinas sejam do mesmo fabricante ou do mesmo tipo. O que realmente é importante é o fato de todas as máquinas poderem ser interligar pela rede, com o mesmo tipo de protocolo de acesso (por exemplo, TCP/IP, NetBEUI).

Podem existir em uma rede vários tipos de servidores e estes podem ser dedicados ou não. Os servidores dedicados têm como vantagens a rapidez na execução de tarefas, segurança nos níveis de acesso, excelente desempenho. Os servidores não dedicados têm como vantagem, em caso de entrar em mau funcionamento ou defeito, os demais terminais continuarão a funcionar normalmente.

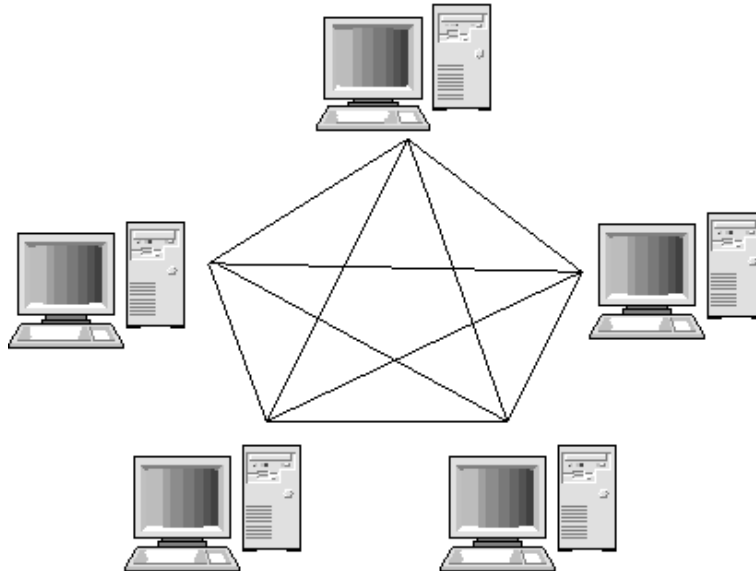
A arquitetura Cliente/Servidor é hoje uma das tecnologias mais utilizadas em ambientes corporativos. Substituindo a arquitetura muito rígida que eram os sistemas envolvendo mainframes. Em ambientes corporativos, o compartilhamento de dados era resolvido através da utilização de mainframes com vários terminais interligados a eles. Estas estruturas, além de ser muito caras, eram muito rígidas.

Com o aumento do poder de processamento dos microcomputadores, os fabricantes de programas para micros começaram a desenvolver banco de dados cada vez mais poderosos, sistemas operacionais mais rápidos e flexíveis, redes LANs e redes WANs. Esta arquitetura mostrou-se mais flexível devido à utilização dos micros em rede, cada vez mais complexos e versáteis, com o compartilhamento de recursos de cada máquina.

Os processos cliente enviam pedidos para o processo servidor, e este por sua vez processa e envia os resultados dos pedidos. Nos sistemas cliente/servidor o processamento tanto do servidor como o do cliente são equilibrados, se for gerado um peso maior em um dos dois lados, provavelmente, esse não seria um sistema cliente/servidor e sim um sistema fracamente acoplado de processamento paralelo.

Geralmente, os serviços oferecidos pelos servidores dependem de processamento específico que só eles podem fazer. O processo cliente, por sua vez, fica livre para realizar outros trabalhos. A interação entre os processos cliente e servidor é uma troca cooperativa, em que o cliente é o ente ativo e o servidor o ente reativo, ou seja, o cliente faz o pedido de uma determinada operação, e neste ponto o servidor processa e responde ao cliente.

Redes Ponto-a-Ponto (Peer-To-Peer)

Geralmente, este tipo de rede é altamente conveniente quando o número de computadores é pequeno assim como também o orçamento. O método oferecido por este tipo de rede é bastante econômico. O tempo de resposta é reduzido sempre que outro usuário estiver compartilhando seus recursos.

É um tipo de sistema de rede no qual cada máquina tem acesso aos recursos de outras máquinas, não é baseada num servidor central. Sua capacidade de processamento é compartilhada com todos os computadores. Normalmente este tipo de rede ponto-a-ponto tem uma topologia do tipo Mesh, já que todas as máquinas estão se enxergando umas com outras, mas qualquer topologia (estrela, barramento, anel) poderia ser também utilizada.

Cabeamento em Redes Ponto-a-Ponto (P2P)

No caso de redes com apenas dois computadores, bastará um único cabo cruzado (Crossed) com conectores RJ-45 para ligar os dois computadores. Este cabo pode ser comprado pronto em lojas de informática, ou feito sob medida (várias lojas confeccionam cabos de rede sob

medida), ou ainda produzido pelo próprio usuário. Se a intenção é apenas formar uma pequena rede com poucos micros, não aconselhamos que seja “criada a infraestrutura” para construir cabos, que consiste no custo do alicate, do cabo, dos conectores e dos diversos conectores inutilizados durante o processo de aprendizado da confecção de cabos.

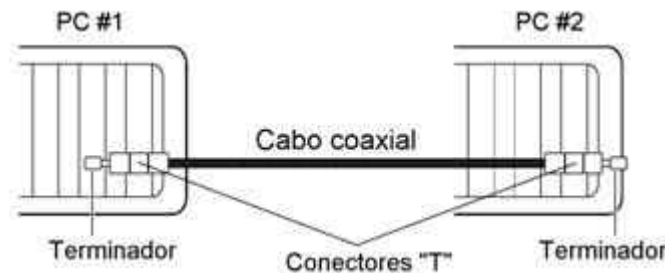
O ideal é usar placas de rede com conectores RJ-45 e com velocidade de 100 Mbps. Nada impede, entretanto que sejam aproveitadas placas mais antigas que operam com apenas 10 Mbps. Note que, neste caso, o desempenho da rede será bastante reduzido, mas ainda assim aceitável para copiar arquivos, compartilhar impressoras e conexões com a Internet.

A transferência de arquivos será cerca de 20 vezes mais demorada que a de um disco rígido moderno, porém 200 vezes mais rápida que uma conexão com a Internet com linha discada. A conexão a 10 Mbps é, portanto bastante adequada para aplicações domésticas e de pequenas empresas. Ainda assim, levando em conta que uma placa de rede de 100 Mbps é bem barato (menos de 50 reais), vale a pena descartar as placas antigas e comprar novas.

Mesmo as placas de rede antigas possuem conectores RJ-45. Alguns modelos, entretanto possuem apenas conectores BNC[2]. Será preciso fazer a ligação entre os dois PCs usando uma seção de cabo coaxial (10BaseT ou 10Base2). Este cabo pode ser comprado em lojas especializadas em equipamentos para redes, juntamente com os conectores “T” e terminadores necessários. A figura mostra como ficaria a conexão entre dois computadores por cabo coaxial. Este esquema pode ser usado para conectar um número maior de computadores.

A rede com este tipo de cabo coaxial não utiliza Hubs, e requer um conector “T” para cada computador e terminadores para serem usados nos dois computadores da extremidade da cadeia. Pode ser vantajoso aproveitar placas de rede antigas para formar uma pequena rede,

[2] Antigamente era comum chamar o conector de redes em barramento com cabo coaxial, de conectores BNC (Bayonet Nipple Connector).

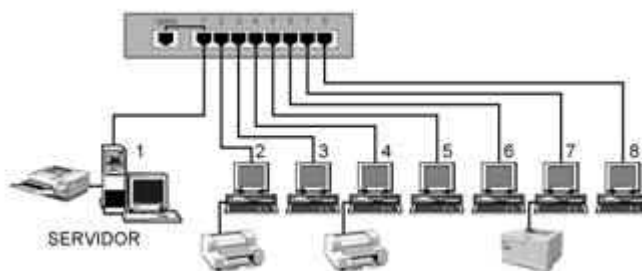
mesmo com a baixa transmissão oferecida pelo cabo 10Base2 e com as dificuldades de expansão próprias deste tipo de cabo. Por outro lado temos a economia resultante de dispensar a compra de placas novas e pela dispensa do uso de Hub.

Existe mais uma desvantagem no aproveitamento de placas antigas. A maioria delas requerem o barramento ISA, não encontrado nos PCs novos. Se for preciso instalar um PC novo nesta rede, terá que ser usada uma placa de rede com conector BNC e com o barramento PCI, o que pode ser muito difícil de encontrar à venda atualmente. Outro problema é que o Windows XP não possui drivers para placas de rede muito antigas, e os fabricantes dessas antigas placas não criaram drivers para o Windows XP. Leve em conta também que essas placas antigas são de difícil instalação, já que não contam com o recurso Plug & Play. Neste sentido os sistemas Linux poderiam ser úteis com placas de rede (com barramento ISA) antigas.

Nosso conselho é descartar as placas de rede antigas e que sejam utilizadas somente novas, que devem ter conector RJ-45 e usarem o barramento PCI. Se a placa de rede for de 10 Mbps, pode ser usada, porém fique preparado para o desempenho baixo.

Uma rede moderna com mais de dois computadores necessita de um Hub ou Switch (a menos que se trate de uma rede sem-fio, que exige outros equipamentos). Quando o tráfego na rede é pequeno podemos usar um Hub, entretanto a diferença entre os preços de Hubs e Switches é atualmente muito pequena, portanto vale a pena optar pelo Switch.

Mesmo em uma rede Ponto-a-Ponto, onde basicamente todas as máquinas são servidores em potencial, nada impede que um dos computadores seja configurado como um servidor dedicado. Se a esmagadora maioria dos acessos à rede é feita entre cada estação e o servidor, então não será possível que no mesmo instante duas ou mais estações tenham

acesso ao servidor (na verdade todas acessam, mas com compartilhamento de tempo, o que reduz o desempenho). Nesta situação, o "gargalo" é o próprio servidor, e não existe diferença entre usar um Hub ou Switch.

Se por outro lado forem comuns os acessos entre estações diferentes (na rede Ponto-a-Ponto, as estações podem operar como servidores), será mais vantajoso utilizar o Switch. Devido ao chaveamento de circuitos do Switch, será possível, por exemplo, o computador 3 enviar dados para a impressora do computador 7 ao mesmo tempo em que o computador 4 acessa um arquivo no computador 8.

Essas transferências são feitas de forma simultânea com o uso do Switch, e cada uma delas terá a taxa de 100 Mbps. Se fossem feitas através de Hub, cada estação teria que esperar sua vez para transmitir seus pacotes de dados, e a taxa de transferência média seria reduzida consideravelmente. Portanto se for a intenção transferir muitos dados entre estações diferentes, o uso do Switch é fundamental para se ter um bom desempenho.

Para redes muito pequenas (por exemplo, uma rede caseira) podem ser usados Hubs ou Switches de 4 ou 8 portas. Tome cuidado, pois Hubs muito baratos normalmente operam com apenas 10 Mbps. Certifique-se de que você está mesmo comprando um Hub ou Switch de 100 Mbps. Essas indicações de velocidade ficam normalmente no próprio painel frontal do dispositivo.

A tabela seguinte resume essas classificações:

Tipos de redes pela abrangência geográfica

TIPO DE REDE	ABRANGÊNCIA GEOGRÁFICA	MÍDIAS UTILIZADAS NA LIGAÇÃO DOS PONTOS
LAN (**L**ocal **A**rea **N**etwork)	Mesma sala, andar, prédio ou conjunto de prédios.	- Cabos (cobre ou fibra óptica) -Ondas de rádio, - Micro-ondas - infravermelho
MAN (**M**etropolitan **A**rea **N**etwork)	Área geográfica como a de uma cidade ou macrorregião	- Ondas de rádio - Microondas - Infravermelho - Linhas telefônicas
WAN (**W**ide **A**rea **N**etwork)	Larga abrangência; Várias cidades distantes, estado ou mesmo países.	- Linhas telefônicas - Canais de satélites

A tabela abaixo mostra os tipos de redes em relação ao número de computadores utilizados.

TIPO DE REDE	COMPUTADORES UTILIZADOS	VANTAGENS	DESVANTAGENS
Cliente/Servidor	- Servidores - Estações cliente	Centralização dos recursos. Suporta redes maiores As estações utilizam todo o seu poder computacional nas tarefas do usuário.	Maior custo envolvido. Um dos computadores é alocado para a tarefa de servidor.
Ponto a ponto	Estações (atuando como servidores ou clientes ou ambos)	Baixo Custo. Não usa um computador exclusivo como servidor.	Suporta apenas redes de pequeno porte. Pode haver perda de desempenho em algumas estações descentralização dos recursos com menor segurança.

Características Necessárias para Implantação

A escolha de um tipo particular de rede para suporte a um dado conjunto de aplicações é uma tarefa difícil. Cada arquitetura possui certas características que afetam sua adequação a uma aplicação em particular. Nenhuma solução pode chamar par si a classificação de ótima quando analisada em contexto geral, e até mesmo em particular. Muitos atributos entram em jogo, o que torna qualquer comparação bastante complexa. Esses atributos dizem respeito

ao custo, à confiabilidade, ao tempo de resposta, à velocidade, ao desempenho, à facilidade de desenvolvimento, à modularidade, à disponibilidade, à facilidade, à complexidade lógica, à facilidade de uso, à facilidade de manutenção, e etc.

O custo de uma rede é dividido entre o custo das estações de processamento (microcomputadores, minicomputadores etc.), o custo das interfaces com o meio de comunicação e o custo do próprio meio de comunicação. O custo das conexões dependerá muito do desempenho que se espera da rede. Redes de baixo a médio desempenho usualmente empregam poucas estações com uma demanda de taxas de dados e volume pequeno, com isso as interfaces serão de baixo custo devido as suas limitações e aplicações.

Redes de alto desempenho já requerem interfaces de custos mais elevados, devido em grande parte ao protocolo de comunicação utilizado e ao meio de comunicação. Várias são as medidas que caracterizam o desempenho de sistemas com isso faz-se necessário definir o que é retardo de transferência, retardo de acesso e retardo de transmissão. É chamado de Retardo de Acesso o intervalo de tempo decorrido desde que uma mensagem a transmitir é gerada pela estação até o momento em que a estação consiga obter somente para ela o direito de transmitir, sem que haja colisão de mensagens no meio.

Retardo de Transmissão é o intervalo de tempo decorrido desde o início da transmissão de uma mensagem por uma estação de origem até o momento em que a mensagem chega à estação de destino. Retardo de Transferência é a soma dos retardos de acesso e transmissão, incluindo o todo o tempo de entrega de uma mensagem, desde o momento em que deseja transmiti-la, até o momento em que ela chega para ser recebida pelo destinatário. O retardo de transferência é, na grande maioria dos casos, uma variável aleatória, no entanto em algumas redes o maior valor que o retardo de transferência pode assumir é limitado, ou seja, (determinístico).

A rede deve ser moldada ao tipo particular de aplicação de modo a assegurar um retardo de transferência baixo. O sistema de comunicação entre os módulos deve ser de alta velocidade e de baixa taxa de erro, de forma a não provocar saturação no tráfego de mensagens. Em

algumas aplicações (em particular as de controle em tempo real) a necessidade de retardo de transferência máximo limitado é de vital importância.

A utilização efetiva do sistema de comunicação é apenas uma porcentagem da capacidade total que ela oferece. Uma rede deve proporcionar capacidade suficiente para viabilizar as tarefas às quais foi destinada. Par tal fim, certos critérios devem ser levados em conta, a escolha adequada da arquitetura, incluindo a estrutura de conexão, o protocolo de comunicação e o meio de transmissão, a velocidade e o retardo de transferência de uma rede são essenciais para um bom desempenho de uma LAN.

A confiabilidade de um sistema em rede pode ser avaliada nos seguintes fatores críticos:

- Do tempo médio entre falhas MTBF (Medium Time Between Failures),
- Da tolerância a falhas ou degradação amena (Gracefull Degradation),
- Do tempo de reconfiguração após falhas e
- Do tempo médio de reparo MTTR (Medium Time To Repair).

O tempo médio entre falhas (MTBF) é geralmente medido em horas, estando relacionado com a confiabilidade dos componentes e nível de redundância. A tolerância a falhas, também conhecida como a degradação amena, depende da aplicação, ela mede a capacidade da rede continuar operando em presença de falhas, embora com um desempenho menor. A reconfiguração após falhas requer (se possível) que caminhos redundantes sejam acionados tão logo ocorra uma falha ou esta seja detectada. A rede deve ser tolerante a falhas transientes causadas por hardware e/ou software, de forma que tais falhas causem apenas uma confusão momentânea que será resolvida sem recursos de redundância, mas essas não são de modo algum as únicas falhas possíveis. O tempo médio de reparo (MTTR) pode ser diminuído com o auxílio de redundância, mecanismos de autoteste e diagnóstico e uma correta manutenção dos equipamentos (HUBs, Switch, roteadores, etc.) da rede.

A modularidade pode ser caracterizada como grau de alteração de desempenho e funcionalidade que um sistema (rede) pode sofrer em mudar seu projeto original. Os três maiores benefícios de uma arquitetura modular são a facilidade para modificação que é simplicidade com funções lógicas ou elementos de hardware podem ser substituídos, a despeito da relação íntima com outros elementos; a facilidade para crescimento diz respeito a configurações de baixo custo, melhora de desempenho e funcionalidade e baixo custo de expansão; e a facilidade para o uso de um conjunto de componentes básicos será melhor facilidade para viabilizar um projeto, adicionar equipamentos à rede, manutenção do sistema como um todo.

Uma rede bem projetada deve poder se adaptar modularmente às várias aplicações para as quais foi projetada, assim como também prever futuras implementações, instalações e atualizações.

É fundamental a compatibilidade utilizada, bem como a capacidade que o sistema (a rede) possui para se ligar aos dispositivos de vários fabricantes, quer em nível de hardware, quer em nível de software. Essa característica é extremamente importante na economia de custo de equipamentos já existentes.

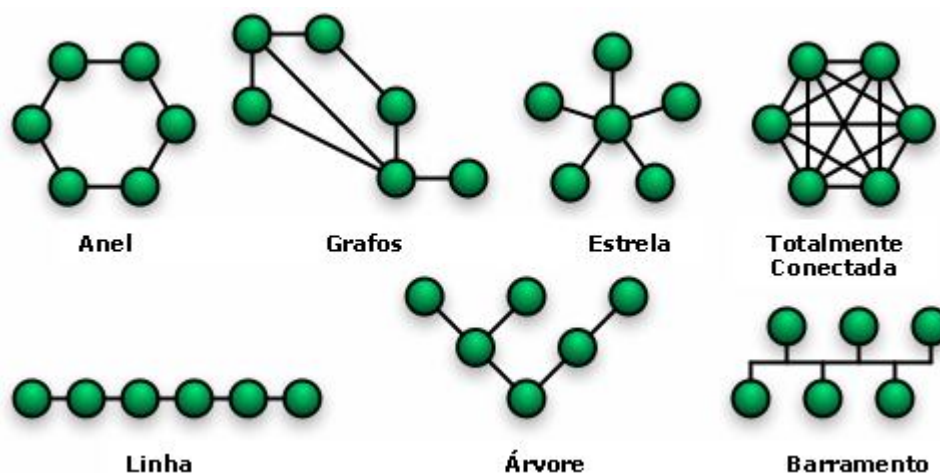
Uma rede deve ter a capacidade de suportar todas as aplicações para as quais foi projetada, e mais aquelas que o futuro possa requer. Quando possível, não deve ser vulnerável à tecnologia, prevendo a utilização de futuros desenvolvimentos, quer sejam novas estações, novos padrões de transmissão ou novas tecnologias de transmissão etc., a isso damos o nome de Sensibilidade Tecnológica.

UNIDADE 8

Objetivo: Conhecer, entender e saber identificar a topologia das atuais redes.

Topologias de Rede

Introdução

Etimologicamente a palavra topologia deriva do grego, **Topos** = forma e **Logos** = estudo, portanto, concluímos que a palavra (ou termo) topologia significa o estudo das formas, das estruturas e como as partes se relacionam com o todo. Essa palavra tem muito uso em várias áreas da Ciência, uma delas é a matemática que estuda os espaços topológicos que se subdividem em Topologia Geral, Topologia algébrica e Teoria das variedades. Porém, aqui não será falado a respeito desses conceitos matemáticos, mas sim sobre a definição que se aplica na área das redes de computadores.

A topologia de uma rede descreve como é o layout (configuração da forma física) do meio através do qual trafegaram os bits de informação, e também como os dispositivos estão conectados um com outros. Há várias formas nas quais se pode organizar as conexões entre cada um dos computadores dentro de uma rede.

No entanto, devemos enfatizar que existem duas topologias em uma mesma rede, que são a topologia física e a topologia lógica que podem ou não ser iguais.

Possuir uma topologia física e lógica é fundamental na construção de qualquer sistema de comunicação. A topologia de uma rede de comunicação irá muitas vezes caracterizar seu tipo, eficiência e velocidade. A topologia física refere-se à forma com que os enlaces físicos e os nós de comunicação estão organizados, determinando os caminhos físicos existentes e utilizáveis entre quaisquer pares de estações conectadas a essa rede.

O “layout físico” constitui o meio de conexão dos dispositivos na rede, ou seja, como estes estão conectados. Os pontos no meio onde são conectados recebem a denominação de nós, sendo que estes nós sempre estão associados a um endereço, para que possam ser reconhecidos pela rede. A topologia lógica refere-se ao modo como as estações da rede irão se comunicar umas com outras, de tal forma de fazer o percurso do fluxo das mensagens. As topologias lógica e física de uma rede podem ser iguais ou diferentes.

Uma rede Token-Ring (IEEE 802.5) é um bom exemplo de uma rede com topologias lógica e física diferentes. Esta tecnologia de rede (proprietária da IBM) utiliza uma topologia física em estrela, com as estações sendo ligadas a dispositivos centrais, denominados MAUs (Multistation Access Units), através de cabos de par trançado. Os MAUs tinham tipicamente 10 portas, sendo 8 para as estações e duas para a ligação com outros MAUs. Portanto fisicamente era possível enxergar uma estrela, mas o fluxo dos quadros entre as estações de uma Token-Ring é feito de forma circular cada estação deve esperar pelo Token para enviar seus dados.

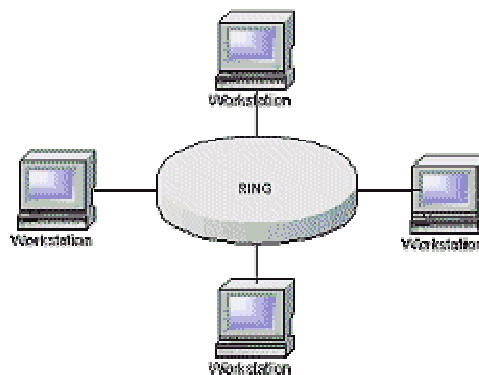
A topologia de uma rede depende do projeto das operações, da confiabilidade e do seu custo operacional. Ao se planejar uma rede, muitos fatores devem ser considerados, mas o tipo de participação dos nodos é um dos mais importantes. Um nodo pode ser fonte ou usuário de recursos, ou uma combinação de ambos.

Topologia Em Anel

Uma rede em anel consiste de estações conectadas através de um caminho fechado. Nesta configuração, muitas das estações remotas ao anel não se comunicam diretamente com o computador central.

Redes em anel são capazes de transmitir e receber dados em qualquer direção, mas as configurações mais usuais são unidirecionais, de forma a tornar menos sofisticados os protocolos de comunicação que asseguram a entrega da mensagem corretamente e em sequencia ao destino.

Quando uma mensagem é enviada por um nó, ela entra no anel e circula até ser retirado pelo nó destino, ou então até voltar ao nó fonte, dependendo do protocolo empregado. O último procedimento é mais desejável porque permite o envio simultâneo de um pacote para múltiplas estações. Outra vantagem é a de permitir, a determinadas estações, receber pacotes enviados por qualquer outra estação da rede, independentemente de qual seja o nó destino.

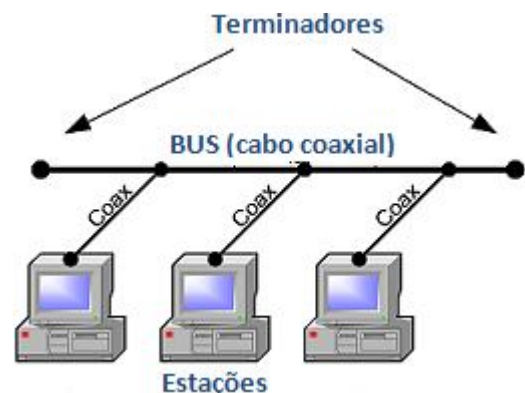
Os maiores problemas desta topologia são relativos à sua pouca tolerância a falhas. Qualquer que seja o controle de acesso empregado, ele pode ser perdido por problemas de falha e pode ser difícil determinar com certeza se este controle foi perdido ou decidir qual nó deve recriá-lo. Os erros de transmissão e processamento podem fazer com que uma mensagem continue eternamente trafegando pelo anel. A utilização de uma estação monitora contorna estes problemas. Outras funções desta estação seriam: iniciar o anel (gerar um novo Token), enviar pacotes de teste e diagnóstico e outras tarefas de manutenção. A estação monitora pode ser dedicada ou outra que assuma em determinado tempo essas funções.

Esta configuração requer que cada nodo seja capaz de remover seletivamente mensagens da rede ou passá-las adiante para o próximo nó. Nas redes unidirecionais, se uma linha entre

dois nodos cair, todo sistema sai do ar até que o problema seja resolvido. Se a rede for bidirecional, nenhum ficará inacessível, já que poderá ser atingido pelo outro lado.

Exemplos clássicos de redes com topologia em anel são: a famosa rede Token-Ring IEEE 802.5 de 4 a 16 Mbps (da IBM) e a rede FDDI (Fiber Distributed Digital Interfase) com 100 Mbps, muito utilizada como Backbones (espinha dorsal) de redes corporativas.

Topologia em Barramento

Nesta configuração todos os nodos (estações) se ligam ao mesmo meio de transmissão. A barra é geralmente compartilhada em tempo e frequência, permitindo transmissão de informação. Nas redes em barra comum, cada nó conectado à barra pode ouvir todas as informações transmitidas. Esta característica facilita as aplicações com mensagens do tipo difusão (para múltiplas estações).

Existe uma variedade de mecanismos para o controle de acesso à barra que pode ser centralizado ou descentralizado. A técnica adotada para acesso à rede é a multiplexação no tempo. Em controle centralizado, o direito de acesso é determinado por uma estação especial da rede. Em um ambiente de controle descentralizado, a responsabilidade de acesso é distribuída entre todos os nodos.

Nas topologias em barramento, as falhas (por desconexão acidental do cabo coaxial, desacoplamento de algum terminador ou placas de rede em mau funcionamento) causam a parada total do sistema. Relógios de prevenção (“watch-dos-timer”) em cada transmissor devem detectar e desconectar o nodo que falha no momento da transmissão. O desempenho de um sistema em barra comum é determinado pelo meio de transmissão, número de nodos conectados, controle de acesso, tipo de tráfego entre outros fatores. O tempo de resposta pode ser altamente dependente do protocolo de acesso utilizado.

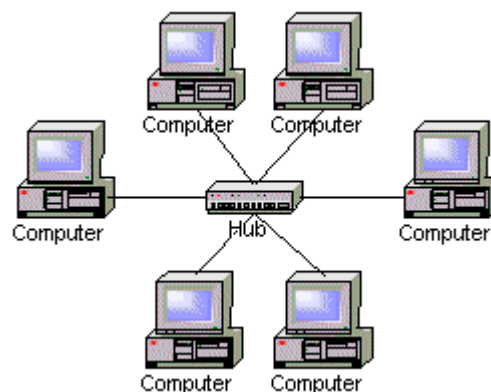
Topologia em Estrela

Neste tipo de rede, todos os usuários se comunicam com um dispositivo central, tem o controle supervisor do sistema, chamado “host”. Através do host os usuários podem se comunicar entre si e com processadores remotos ou terminais. No segundo caso, o host funciona como um comutador de mensagens para passar os dados entre eles.

O arranjo em estrela é a melhor escolha se o padrão de comunicação da rede for de um conjunto de estações secundárias que se comunicam com o nodo central. As situações onde isto mais acontece são aquelas em que o nodo central está restrito às funções de gerente das comunicações e a operações de diagnósticos. O gerenciamento das comunicações por este nó central pode ser por chaveamento de pacotes ou de circuitos.

O nó central poderia realizar outras funções além das de chaveamento e processamento normal. Por exemplo, pode compatibilizar a velocidade de comunicação entre o transmissor e o receptor. Pode-se dar o caso do nó central atuar como um conversor de protocolos, permitindo duas redes de fabricantes diferentes se comunicarem sem problemas, em situações normais, esta última tarefa geralmente é confinada aos roteadores de rede.

No caso de ocorrer falha em uma estação ou na conexão com o nodo central, apenas esta estação fica fora de operação. Entretanto, se uma falha ocorrer no nodo central, todo o sistema pode ficar fora do ar. A solução deste problema seria a redundância, mas isto acarreta um aumento considerável dos custos.

A expansão de uma rede deste tipo de rede só pode ser feita até um certo limite, imposto pelo nodo central em termos da capacidade de chaveamento, número de circuitos concorrentes que podem ser gerenciados e número de nós que podem ser servidos. O desempenho obtido numa rede em estrela depende da quantidade de tempo requerido pelo nodo central para processar e encaminhar mensagens, e da carga de tráfego de conexão, ou seja, é limitado pela capacidade de processamento do nodo central. Esta configuração

facilita o controle da rede (e a maioria dos sistemas de computação) com funções de comunicação possuem um software que implementa esta configuração.

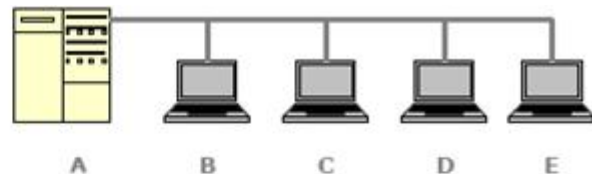
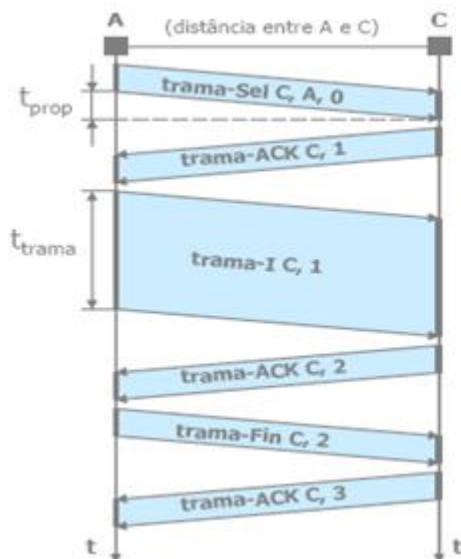
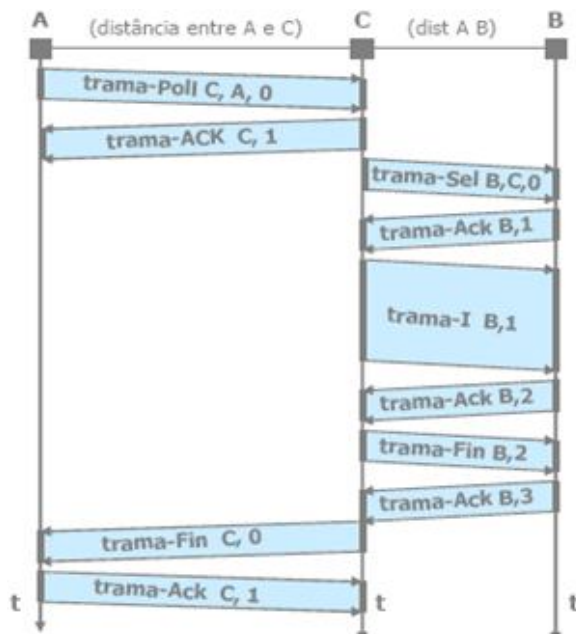
Abaixo segue um quadro comparativo das topologias:

Topologias Básicas	Vantagens	Desvantagens
Topologia Estrela (FastEthernet)	É mais tolerante a falhas, fácil de instalar novos usuários, tem monitoramento centralizado.	Custo de instalação maior porque recebe mais cabos
Topologia Anel (Token-Ring)	Razoavelmente fácil de instalar, requer menos cabos, desempenho uniforme.	Se uma estação para, então todas as outras também param, mas é fácil de isolar o problema.
Topologia em Barramento (Ethernet)	Simples e fácil de instalar Requer menos cabos, fácil de entender a estrutura da rede.	A rede fica mais lenta em períodos de uso intenso. Às vezes, os problemas são difíceis de isolar.

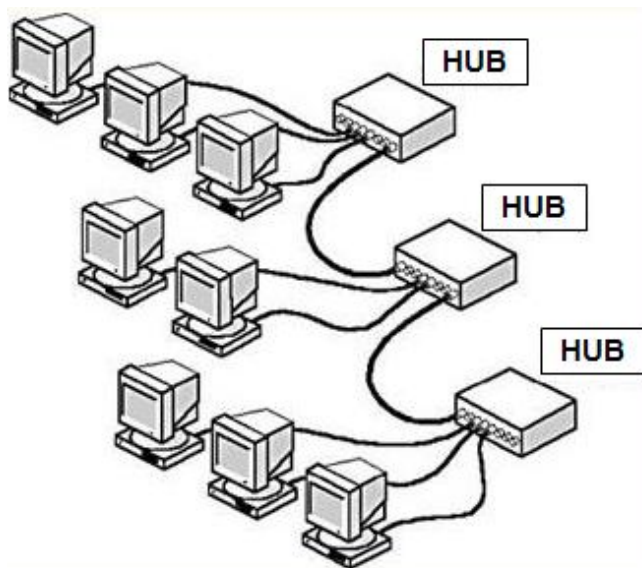
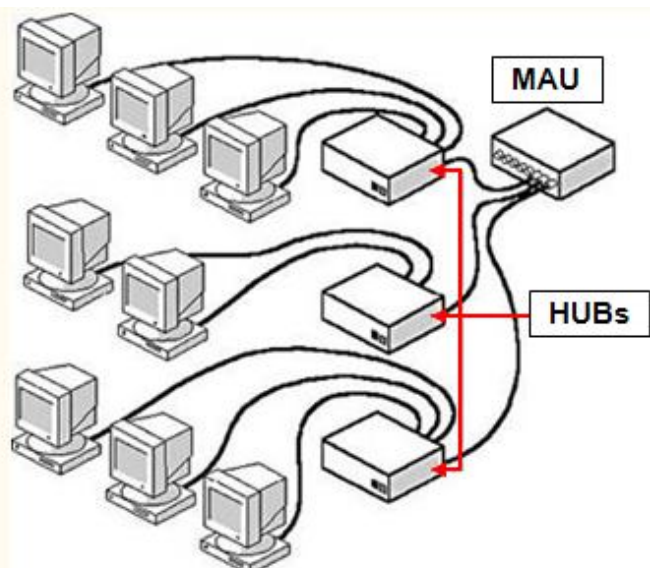
Topologia Multiponto

Nesta modalidade de ligação existe sempre uma estação controladora que coordena o tráfego de dados das demais estações chamadas subordinadas. Este controle é feito através de uma rotina de atendimento denominada “POLL-SELECT”. Neste tipo de redes o computador mestre (ou principal) passa o controle (Poll) para uma estação secundária ficando esta autorizada a selecionar outra estação para enviar dados.

Estas redes podem permitir que estações subordinadas se comuniquem entre si diretamente ou apenas através da estação controladora. A diferença entre estes dois modos de envio de mensagens é a complexidade do algoritmo de controle.

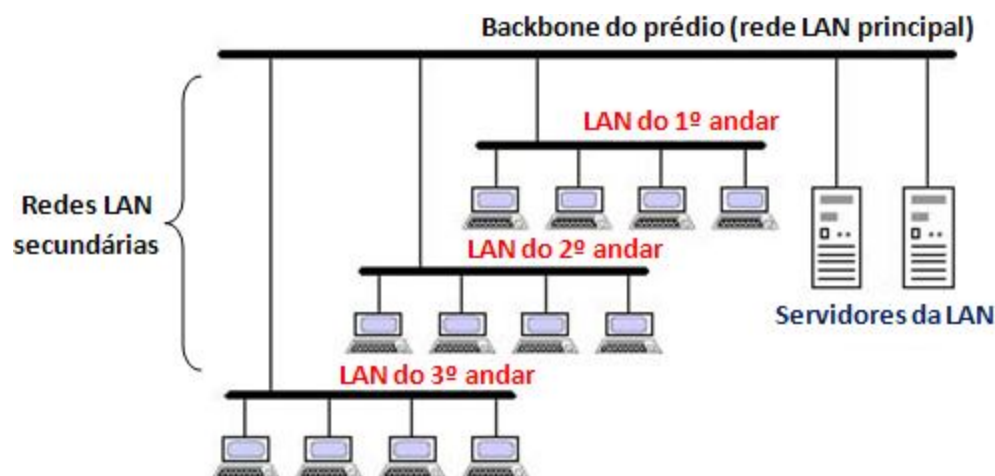
A seguir mostra-se um exemplo da rotina de atendimento POLL-SELECT:

- **Considere-se que a estação (A) é a primária e que as restantes são estações secundárias**
- **A estação primária (A) selecciona a estação secundária (C) para lhe enviar dados**
- **Diz-se que (A) estabelece uma ligação lógica com a estação (C)**

- **A estação primária (A) faz Polling à estação secundária (C) para lhe dar o control da linha**
- **A estação secundária (C) passa a comportar-se como primária e estabelece uma ligação lógica com a estação secundária (B) para lhe enviar dados**
- **Ao terminar a ligação com (B), a estação (C) devolve o control da linha à estação primária (A)**

Topologias Mistas

As estruturas mistas são tipos de redes que utilizam características dos dois tipos básicos de redes, a ligação ponto-a-ponto e multiponto, para obter redes mais complexas e com maiores recursos. As estruturas mistas podem ser do tipo Estrela, Barra e Anel.

Topologia Hierárquica

Este tipo de topologia também é conhecida como a topologia em árvore. Ela se caracteriza por uma série de barras interconectadas com uma barra central. Cada ramificação significa que a informação deverá se conduzir por dois caminhos diferentes. Esta topologia é muito usada atualmente em grandes corporações, tais como Bancos e grandes empresas como algumas de automação industrial. Basicamente uma rede com topologia hierárquica é composta de uma rede principal conhecida como o Backbone da empresa, nesse Backbone (normalmente) se encontram conectados os servidores de rede assim como também as redes LAN secundárias da corporação.

A topologia em árvore é essencialmente uma série de barras interconectadas. Geralmente existe uma barra central, ou seja, um caminho principal chamado de backbone e outros ramos (caminhos secundários) menores são conectados a ele. Esta ligação é realizada através de derivadores e as conexões das estações realizadas do mesmo modo que no sistema de barra padrão.

Cuidados adicionais devem ser tomados nas redes em árvores, pois cada ramificação significa que o sinal deverá se propagar por dois caminhos diferentes. A menos que estes caminhos estejam perfeitamente casados, os sinais terão velocidades de propagação diferentes e refletirão os sinais de diferentes maneiras. Por estes motivos as redes em árvore podem trabalhar com taxas de transmissão menor do que as redes em barra comum. Atualmente não se tem quase redes com este tipo de topologia em árvore.

Topologia de Grafos

A topologia mais geral de redes locais é a estrutura de grafos também conhecida como redes parcialmente ligadas. Desta derivam as redes completamente ligadas, as redes parcialmente ligadas, em estrela e as redes em anel. Redes interligadas ponto-a-ponto crescem em complexidade com o aumento do número de estações conectadas.

Nestes sistemas não é necessário que cada estação esteja ligada a todas as outras (sistemas completamente ligados). Devido ao custo das ligações é mais comum o uso de sistemas parcialmente ligados baseados em chaveamento de circuitos de mensagens ou de pacotes. O arranjo das ligações é baseado normalmente no volume de tráfego na rede.

A generalidade introduzida neste tipo de topologia tem por objetivo a otimização do custo do meio de transmissão. Devido a isto tal topologia é normalmente empregada em redes de longas distâncias, isto é, redes geograficamente distribuídas.

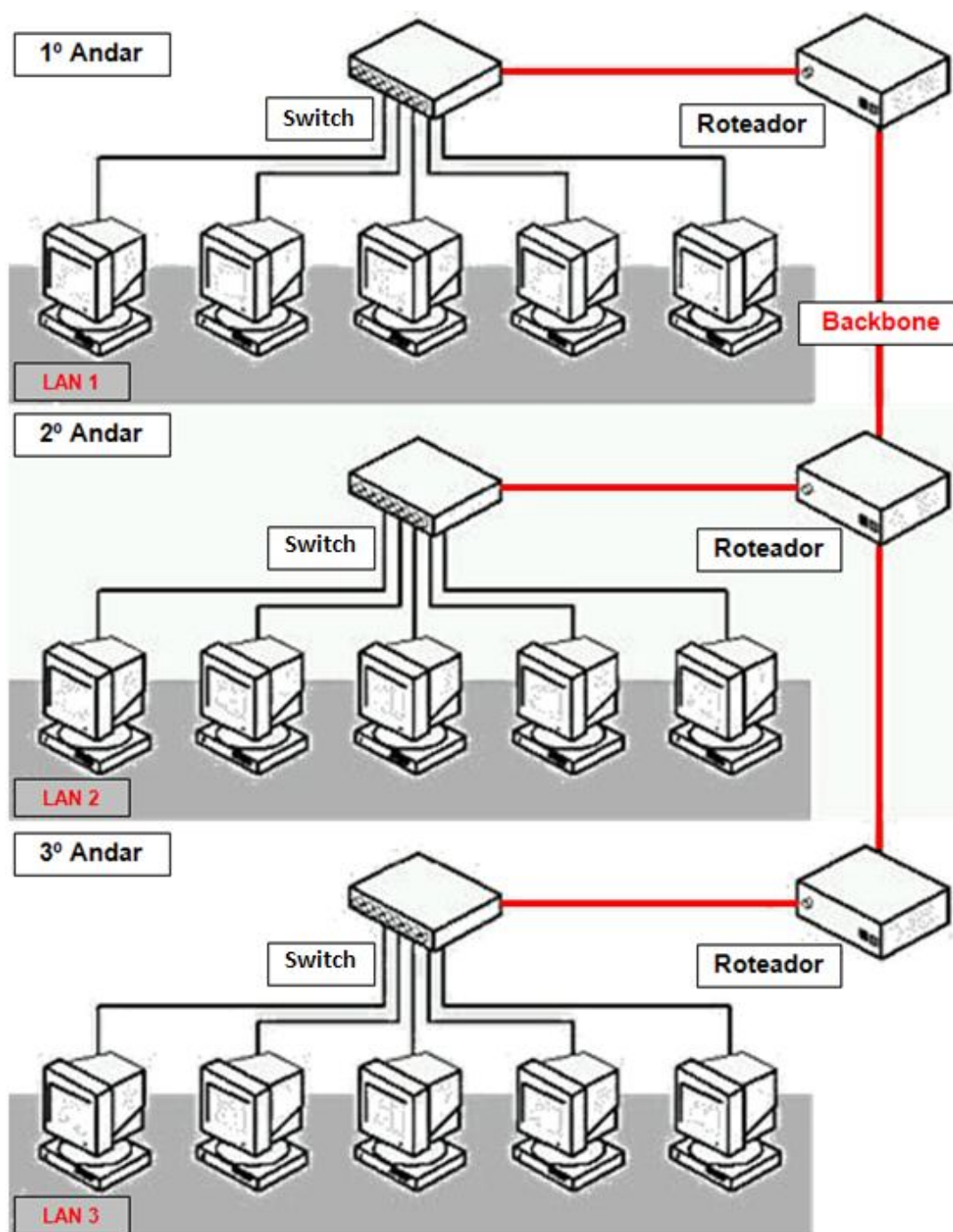
Em redes LAN meios de transmissão de alta velocidade e privados podem ser utilizados, pois têm um custo baixo, devido às limitações das distâncias impostas. Tal topologia não tem tanta aplicação neste caso, já que devido a sua generalidade, introduz complexos mecanismos para tomar decisões de roteamento em cada nó da rede. Tais mecanismos iriam introduzir um custo adicional nas interfaces de rede que tornariam seu uso proibitivo quando comparado com o custo das estações.

As estruturas parcialmente ligadas têm o mesmo problema de confiabilidade das estruturas em anel. O problema, no entanto, é atenuado devido à existência de caminhos alternativos em caso de falha de um nó principal. A modularidade desta topologia é boa desde que dois ou mais nós (com os quais um novo nó a ser incluído se ligaria) possam suportar o aumento do carregamento.

Relação entre Topologia e Meios de Transmissão

Certas topologias estão ligadas a unidirecionalidade (ou bidirecionalidade) do meio de transmissão. Fora esse fator, teoricamente, qualquer meio de transmissão pode ser usado em qualquer topologia. Mas o estágio atual do desenvolvimento tecnológico só permite que algumas combinações sejam usadas nas redes locais comercializadas hoje, pois o custo de outras combinações é proibitivo para o estado atual da arte.

A topologia em barra emprega como meio de transmissão os cabos coaxiais de 50 Ohms. Exemplos de rede em barramento são as redes Ethernet (IEEE 802.3) de 10 Mbps. Não é

economicamente vantajoso usar fibra óptica em ligações multiponto de redes locais. A topologia em anel pode ser construída com par trançado, cabos de 50 Ohms. O uso do cabo de 75 Ohms exigiria um número elevado de repetidores para múltiplos canais, o que o tornaria economicamente inviável.

Atualmente a topologia em estrela está sendo muito viável para taxas de transmissão elevadas, por exemplo, as redes com arquitetura FastEthernet 802.3u de 10/100 Mbps, o que nos leva a escolher esta topologia, com cabos de par trançado UTP, como um meio de transmissão bastante adequado.

Segue a tabela entre topologia e meio de transmissão

Meio de Transmissão	Barramento	Anel	Estrela	Arvore
Par Trançado (UTP, STP)	X	X	X	
Coaxial 50 Ohms	X	X		
Coaxial 75 Ohms	X			X
Fibra Óptica		X		

Abaixo segue um quadro comparativo das topologias:

Características	Estrela	Anel	Barramento	Grafos
Simplicidade Funcional	A melhor de todas.	Razoável	Razoável, um pouco melhor do que o anel.	Extremamente complexa.
Roteamento	Depende do dispositivo central.	Alto e confiável. Unidirecional no sentido do Token.	Por difusão.	Bastante complexo
Custo de Conexão	Baixo (incluindo cabos, Hub/Switch e conectores).	Baixo para médio	Baixo para médio	Muito alto
Crescimento Incremental	Limitado ao número de portas	Teoricamente infinito	Alto	Alto

	do Hub/Switch central.			
Aplicação Adequada	Redes LAN de médio e grande porte.	Sem limitação	Sem limitação	Sem limitação
Desempenho	Alto, embora todas as mensagens devam passar pelo Hub/Switch central.	Alto, possibilidade de mais de uma mensagem ser transmitida ao mesmo tempo.	Médio, mais de uma mensagem pode ser transmitida ao mesmo tempo ocasionando colisões.	Alto. Pode se adaptar ao volume de tráfego existente
Confiabilidade	Pouca confiabilidade	Boa, desde que sejam tomados cuidados adicionais.	A melhor de todas. Interface passiva com o meio.	Boa, devido à existência de caminhos alternativos.
Retardo de Transmissão	Médio	Baixo, podendo chegar a não maior da duração de 1 bit por nó.	Mais baixo de todas	Alto
Limitação quanto ao Meio de Transmissão	Nenhuma. Ligação ponto a ponto	Nenhuma. Ligação ponto a ponto	Limitado. Por ter a ligação multiponto sua ligação ao meio de transmissão é feita por difusão (ou Broadcasting), sobre todo com as redes Ethernet.	Nenhuma. Ligação ponto a ponto

UNIDADE 9

Objetivo: Conhecer os principais tipos de cabos que fazem a conexão das redes.

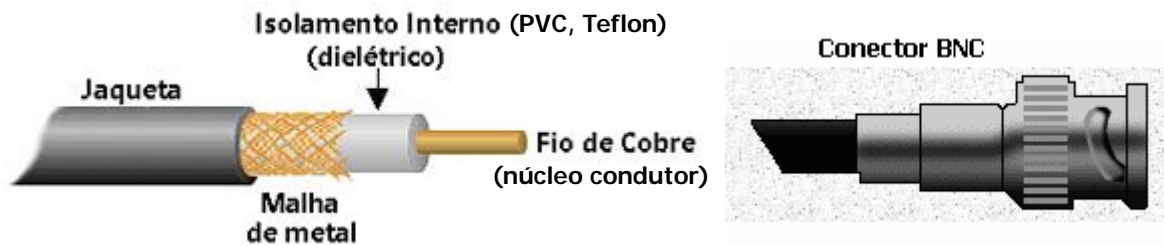
Cabeamento De Redes (Parte I)

Abaixo seguem os principais tipos de cabos utilizados nas redes de computadores:

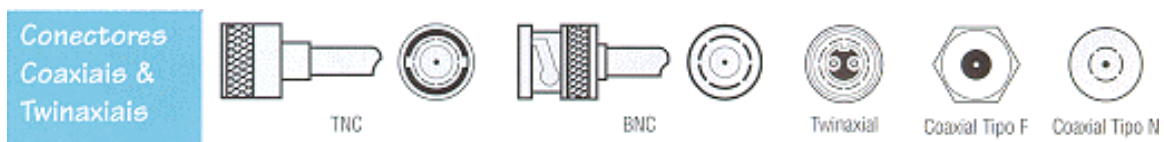
- Cabo coaxial;
- Cabo de par trançado não blindado UTP (Unshielded Twisted Pair);
- Cabo de par trançado com blindagem STP (Shielded Twisted Pair);
- Cabo de fibra óptica.

Cabo Coaxial

Na década dos 80/90 surgiu o cabo coaxial e naquela época era o que havia de mais avançado, sendo que a troca de dados entre dois computadores era coisa do futuro. Até hoje existem vários tipos de cabos coaxiais, cada um com suas características específicas. Alguns são melhores para transmissão em alta frequência, outros têm atenuação mais baixa, e outros são imunes a ruídos e interferências.

Os cabos coaxiais de alta qualidade não são maleáveis e são difíceis de instalar e os cabos de baixa qualidade podem ser inadequados para trafegar dados em alta velocidade e longas distâncias. Ao contrário do cabo de par trançado, o coaxial mantém uma capacidade constante e baixa, independente do seu comprimento, evitando assim vários problemas técnicos. Devido a isso, ele oferece velocidade da ordem de Mbps, não sendo necessária a regeneração do sinal, sem distorção ou eco, propriedade que já revela alta tecnologia. O cabo coaxial pode ser usado em ligações ponto-a-ponto ou multiponto.

A ligação do cabo coaxial causa reflexão devido à impedância não infinita do conector. A colocação destes conectores, em ligação multiponto, deve ser controlada de forma a garantir que as reflexões não desapareçam em fase de um valor significativo.

A maioria dos sistemas de transmissão (utilizando banda base) faz uso de cabos coaxiais com uma impedância características de 50 Ohms, geralmente utilizados também nas TVs a cabo e em redes de banda larga. Isso se deve ao fato de a transmissão em banda base sofrer menos reflexões, devido às capacitâncias introduzidas nas ligações ao cabo de 50 Ohms.

Os cabos coaxiais possuem uma maior imunidade a ruídos eletromagnéticos de baixa frequência e, por isso, eram o meio de transmissão mais usado em redes locais.

O cabo coaxial consiste em um condutor cilíndrico externo que circunda um fio interno feito de dois elementos condutores. Um desses elementos, localizados no centro do cabo, é um condutor de cobre. Em volta, há uma camada de isolamento flexível. Sobre esse material de isolamento, há uma malha de cobre ou uma folha metálica que funciona como o segundo fio no circuito e como uma blindagem para o condutor interno. Essa segunda camada, ou blindagem pode ajudar a reduzir a quantidade de interferência externa. Cobrindo essa

blindagem, está o revestimento do cabo. O cabo coaxial é mais caro de se instalar do que o cabo de par trançado.

Abaixo segue uma tabela com os tipos de cabos coaxiais:

Tipo de Cabo	Impedância	Diâmetro	Conector
Cabo fino Ethernet (RG-58)	50 Ohms	3/16"	BNC
ARCNET – RG-62	93 Ohms	3/16"	BNC
ARCNET – RG-59/U	75 Ohms	3/16"	Utiliza um rabicho RG-62 na extremidade com BNC
Cabo Ethernet grosso (Thick Ethernet)	50 Ohms	1/2"	Transceptor/MAU no cabo espesso com uma derivação de par trançado até o cordão da rede
Cabo derivado do cabo Ethernet grosso (não é coaxial, é um cabo de par blindado).	-	3/8"	DIX/AUI

Algumas desvantagens do cabo coaxial são:

- Necessita manter a impedância constante ao longo de todo o segmento através de terminadores.
- Se o cabo coaxial quebrar, ou o conector "T" de interligação estiver com mau contato, toda a rede para de funcionar devido ao desacoplamento de impedâncias do cabo, isto é, no ponto de quebra o sinal encontra uma impedância elevadíssima (quase infinita) se comparada coma impedância nominal do cabo (50 ou 75 Ohms), isto faz

com que o sinal elétrico retorne gerando assim ondas estacionárias que impossibilitam o funcionamento normal da rede.

- Blindagem feita com a malha do cabo, que deverá estar aterrada em todos os terminais, ocasionando diferentes potenciais elétricos. A blindagem acaba funcionando como uma antena captando ruído de radiofrequência.
- Se esta blindagem for aterrada num ponto do edifício, e em outro ponto a 100 m do 1º ponto, com certeza esta blindagem terá potenciais diferentes, ocasionando correntes elétricas pela malha entre os micros. Nesta condição, se uma descarga atmosférica ocorrer próxima a 500m do 1º ponto elevará o potencial de terra do 1º ponto a um valor muito maior do que no 2º ponto a 100m, gerando um pico de tensão pelo cabo do 1º ao 2º ponto, com potencial de até 1.000 Volts, podendo danificar diversos terminais e até mesmo o servidor com consequências graves para a nossa rede.
- É um cabo muito pesado e de difícil instalação.
- Terminais, cabos e conectores relativamente caros.

Cabo De Par Trançado (UTP e STP)

Com o passar do tempo, surgiu o cabeamento utilizando o par trançado. Esse tipo de cabo tornou-se muito usado devido à falta de flexibilidade de outros cabos e por causa da necessidade de se ter um meio físico que conseguisse uma taxa de transmissão alta e mais rápida. Os cabos de par trançado possuem dois ou mais fios entrelaçados em forma de espiral e, por isso, reduzem o ruído e mantém constantes as propriedades elétricas do meio, em todo o seu comprimento.

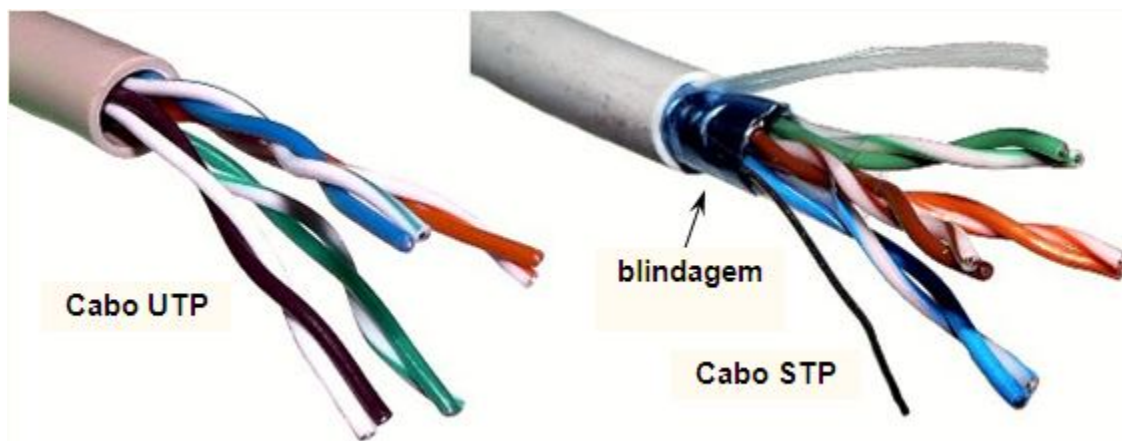
A desvantagem deste tipo de cabo, que pode ter transmissão tanto analógica quanto digital, é sua suscetibilidade às interferências a ruídos (eletromagnéticos e radiofrequência). Esses efeitos podem, entretanto, ser minimizados com blindagem adequada. Vale destacar que

várias empresas já perceberam que, em sistemas de baixa frequência, a imunidade a ruídos é tão boa quanto à do cabo coaxial.

O cabo de par trançado é o meio de transmissão de menor custo por comprimento no mercado. A ligação de nós ao cabo é também extremamente simples e de baixo custo. Esse cabo se adapta muito bem às redes com topologia em estrela, onde as taxas de dados mais elevadas permitidas por ele e pela fibra óptica ultrapassam, e muito, a capacidade das chaves disponíveis com a tecnologia atual. Hoje em dia, o par trançado também está sendo usado com sucesso em conjunto com sistemas ATM para viabilizar o tráfego de dados a uma velocidade extremamente alta.

1. **Par trançado sem blindagem UTP (Unshilded Twisted Par)**: O cabo de par trançado não blindado (UTP) é constituído por pares de cabos trançados. Cada par de fios é isolado dos outros. Esse cabo usa apenas o efeito de cancelamento, produzido pelos pares de fios trançados para limitar a degradação do sinal causada por interferência eletromagnética e por interferência da frequência de rádio. Para reduzir ainda mais a diafonia entre os pares no cabo UTP, o número de trançamentos nos pares de fios varia. O cabo de par trançado não blindado (UTP) tem muitas vantagens. Ele é fácil de ser instalado e mais barato, pois custa menos por metro do que qualquer outro tipo de cabeamento de LAN, no entanto, o que realmente é vantajoso é a sua espessura. Como tem o diâmetro externo pequeno, o UTP não enche os dutos de cabeamento tão rapidamente quanto outros tipos de cabos. Esse pode ser um fator muito importante para se levar em conta, particularmente quando se instala uma rede em um prédio antigo. Além disso, quando o cabo UTP é instalado usando-se um conector RJ, fontes potenciais de ruído na rede são muito reduzidas e uma conexão bem sólida é praticamente garantida. Atualmente o UTP é considerado o mais veloz meio baseado em cobre.

2. **Par trançado com blindagem STP (Shilded Twisted Par)**: O cabo STP combina as técnicas de blindagem, cancelamento e trançamento de fios. Conforme especificado para uso nas instalações de rede Ethernet, o STP fornece resistência à interferência eletromagnética e à interferência de frequência de rádio sem aumento significativo do

peso ou do tamanho do cabo. O cabo de par trançado blindado tem todas as vantagens e desvantagens do cabo de par trançado não blindado. No entanto, o STP permite maior proteção contra todos os tipos de interferências externas, porém é mais caro do que o cabo de par trançado não blindado. O cabo STP é muito pouco utilizado sendo basicamente necessários em ambientes externos com grande nível de interferência eletromagnética. Deve-se dar preferência a sistemas com cabos de fibra óptica quando se deseja grandes distâncias ou velocidades de transmissão, podem ser encontrados com blindagem simples ou com blindagem par a par.

Há, no entanto, desvantagens no uso de cabeamento de par trançado. O cabo UTP é mais propenso ao ruído elétrico e à interferência do que outros tipos de cabos. A distância entre os repetidores de sinais é menor para o UTP do que para o cabo coaxial. Devido a estas limitações do cabo coaxial, o Comitê de normalização Internacional IEEE formado pelas empresas americanas Electrical Industrial American (EIA), e as Telecomunications Industrial American (TIA), se uniram no intuito de pesquisar e produzir um meio de comunicação eficiente e seguro para as Redes de computadores. Desenvolvendo o Standard 10BaseT em 1988. Surgiu assim, na Bell Laboratories o cabo UTP.

A teoria é que, um par de fios torcidos cria uma espira virtual com capacitância e indutância, suficientes para ir cancelando o ruído externo através de suas múltiplas espiras, ou seja, o campo magnético formado pela espira X é reverso da espira Y, e assim por diante. Se em determinado momento o cabo sofrer uma interferência, esta será anulada na inversão dos pólos das espiras. O ruído é cancelado pela mudança de polaridade do sinal através das

múltiplas espiras. Atualmente os cabos UTPs são fabricados com 4 (quatro) pares, ou seja, 4 (quatro) fios torcidos dentro de um único cabo.

O cabo UTP oferece algumas vantagens conforme descrito abaixo:

- Não tem blindagem, portanto não necessita de Aterramento.
- Mantém impedância constante de 100 Ohms sem terminadores.
- Cabo leve, fino, de baixo valor por metro e de conectores baratos.
- No cabeamento estruturado para o cabo UTP, quando há mau contato ou o cabo é interrompido, apenas um micro pára de funcionar, enquanto o resto da Rede continua funcionando normalmente.
- Permite taxas de Transmissão da ordem de 155 Mbps por par.
- Alcança velocidades de 155 Mbps a 622 Mbps ATM ou FastEthernet 100 Mbps.

Abaixo segue um quadro com as classificações do cabo par trançado:

Tipo	Velocidade	Mídia do Cabo	Conector	Uso
Categoria 1	Não adequada a LANs			

Categoria 2	Não adequada a LANs			
Categoria 3	Até 10 Mbps	UTP 4 pares 100 Ohms	568A ou 568B de 8 fios	10BaseT
Categoria 4	Até 16 Mbps	STP 2 pares 150 Ohms	STP-A	10BaseT ou Token-Ring
Categoria 5	Até 100 Mbps	UTP 4 pares 100 Ohms	568A ou 568B de 8 fios	10BaseT, 100Base-T, FDDI, ATM, Token-Ring

Conectores utilizados e esquema de crimpagem dos pares:

RJ-45 macho (Cat. 5)

RJ-45 fêmea (Cat. 5e)

Normas TIA/EIA 568-A

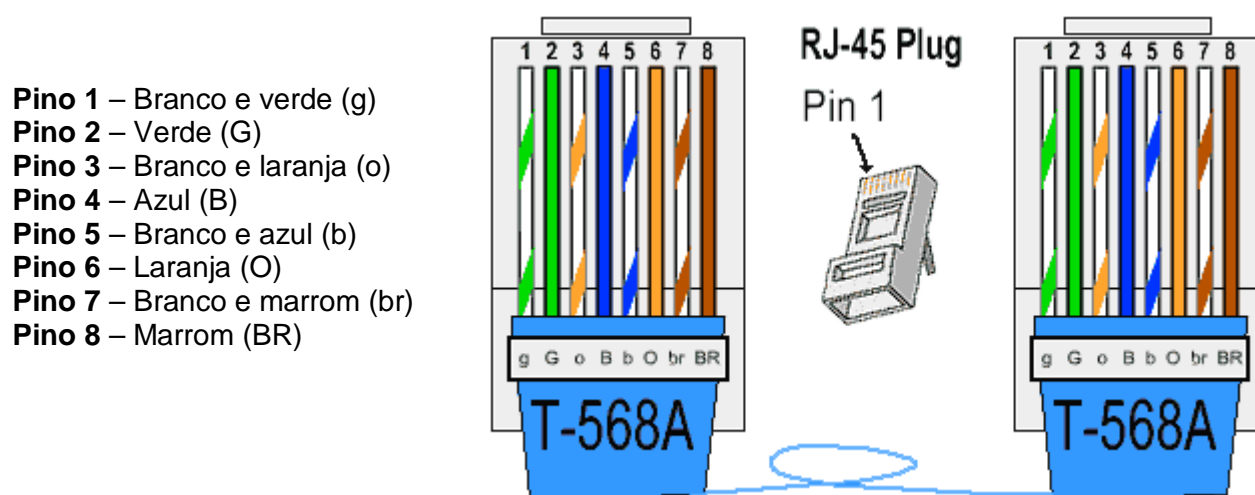
Um Guia de Referência sobre as normas de cabeamento de Telecomunicações para Edifícios Comerciais. Com o crescimento do uso das redes locais de computadores e a agregação de novos serviços ditos multimídia acabaram ditando a necessidade de se

estabelecer critérios para ordenar e estruturar do cabeamento dentro das empresas. Assim, normas e procedimentos forma propostos por comitês como os da EIA/TIA e da ISO/IEC.

Aqui discutimos os aspectos introdutórios do sistema de cabeamento estruturado. A seguir é apresentado o tratamento do código de cores para sistema de cabeamento UTP para redes LAN de alta velocidade.

Código De Cores Para Sistemas De Cabeamento UTP

A EIA/TIA 568A define um sistema de codificação com quatro cores básicas, em combinação com o branco, para os condutores UTP de 100 Ohms, assim como a ordem dos pares no conector RJ-45, conforme ilustrado na figura. Código de cores do cabeamento UTP 100 Ohms segundo o padrão EIA/TIA 568A. Pinagem da esquerda para a direita com os "contatos" dourados de frente para você:

Pino 1 – Branco e verde (g)
Pino 2 – Verde (G)
Pino 3 – Branco e laranja (o)
Pino 4 – Azul (B)
Pino 5 – Branco e azul (b)
Pino 6 – Laranja (O)
Pino 7 – Branco e marrom (br)
Pino 8 – Marrom (BR)

Ordem dos 4 pares de fios no conector RJ-45 padrão T-568A:

- **Par 1**: pinos 4 e 5
- **Par 2**: pinos 3 e 6

- **Par 3**: pinos 1 e 2
- **Par 4**: pinos 7 e 8

O par trançado é o meio de transmissão de menor custo por comprimento. A ligação de nós ao cabo é extremamente simples, portanto de baixo custo. A desvantagem é sua susceptibilidade à interferência e ruído, incluindo "Cross-talk" de fiação adjacente. Em sistema de baixa frequência a imunidade a ruído é tão boa quanto ao cabo coaxial.

Além do cabo UTP, as pesquisas levaram à criação da fibra óptica, um tarugo de 10 cm. de quartzo (cristal), que é estirado até alcançar um comprimento de 2Km a 20Km, com uma espessura de um fio de cabelo, capaz de transmitir dados em forma de luz, internamente a uma velocidade de aproximadamente 2.500 Mbps ou mais (não há aparelhos hoje acima desta velocidade). A fibra óptica pode trafegar livre de interferência e de espúrios atmosféricos, sem blindagem e sem aterramento.

Com estes novos componentes as empresas americanas EIA/TIA criaram as seguintes normas para as Redes de Computadores (telefonia e imagem), vejamos:

- **TIA/EIA-568A**: Padrão de cabeamento para telecomunicações de prédios comerciais.
- **TIA/EIA-569A**: Padrão para espaços e caminhos para telecomunicações de prédios comerciais.
- **TIA/EIA-570A**: Padrão de fiação para telecomunicações residenciais e comerciais leves.
- **TIA/EIA-606**: Padrão de administração para a infraestrutura de telecomunicações de prédios comerciais.
- **TIA/EIA-607**: Requisitos de aterramento e conexões de prédios comerciais para telecomunicações.

A Norma EIA/TIA-568A, garante comunicação de dados até 100m para o cabo UTP, a velocidades de 100 Mbps (categoria 5) que atualmente é muito utilizado e ainda é o estado da arte, e 2.500 Mbps para fibras até 2.500m (multímodo) e 60.000m (mono modo).

Segundo o modelo ISO/OSI, o Ethernet é o padrão que define os níveis 1 e 2 (físico e lógico) especificados pelas normas 802.3 e 802.2 IEEE. O cabo UTP garante 155 Mbps por par, ou seja, 4 x 155 Mbps = 622 Mbps, pois tem 4 (quatro) pares. Este é o cabeamento estruturado, pois pode trafegar a qualquer velocidade, desde 0,1 MHz a 100 MHz, atendendo todas as categorias: Cat. 3 (10 Mhz), Cat. 4 (até 20 Mhz), substituída pela Cat. 5 (100 Mhz).

Cabos Categoria 6 (UTP)

Muito embora a categoria 5 seja altamente utilizada no projeto de cabeamento de redes, existe já a categoria 6. Em junho de 2002, foi aprovado e publicado o adendo número 1 da norma ANSI/TIA/EIA-568-B.2 – "Transmission Performance Specifications for 4-Pair 100 Ohms Category 6 Cabling", contendo todas as especificações necessárias com os requerimentos mínimos para perda de inserção, NEXT (Near-end Crosstalk), FEXT (Far-end Crosstalk), perda de retorno, retardo de propagação, etc. para o cabeamento e o hardware de conexão Categoria 6. O documento contém especificações finais da Categoria 6, as especificações de componentes e requerimentos para equipamentos de teste que garantem o desempenho da rede nas tecnologias atualmente conhecidas, bem como para aplicações futuras.

A Categoria 6 pode ser vista como um aperfeiçoamento no projeto de infraestrutura das redes locais. Ela segue seus predecessores, as categorias 3, 4, 5 e 5e, cada uma provendo maior capacidade de transporte de informação para usuários finais. Torna-se uma opção que oferece alto desempenho para a distribuição horizontal em um sistema estruturado, permitindo suporte para aplicações como voz tradicional (telefone analógico ou digital), VoIP, Ethernet (10BaseT), Fast Ethernet (100Base-TX) e Gigabit Ethernet a 4 pares (1000Base-T), com melhor performance em relação a Categoria 5e. Ela permite ainda suporte para

aplicações ATM e novas tecnologias como Ethernet a 10Gbps sem investimentos adicionais na infraestrutura existente.

Os sistemas Categoria 6 foram projetados para atender basicamente os seguintes objetivos:

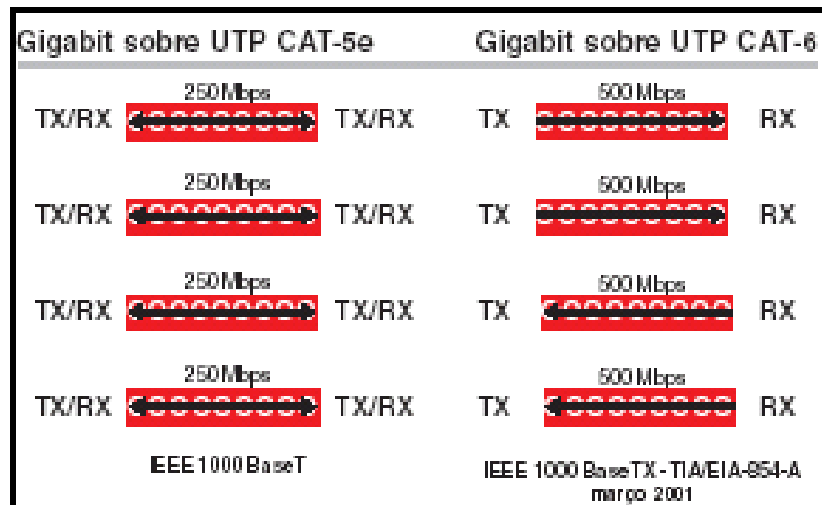
- Manter boa relação custo x benefício dos sistemas UTP, bem como facilitar sua instalação e operação.
- Garantir a interoperabilidade com os atuais sistemas Categoria 5e.
- Proporcionar uma nova infraestrutura com capacidade para serviços futuros (redes de próxima geração).

Aplicações Dos Cabos Cat. 6 (UTP)

Todas as aplicações que funcionam atualmente em Categoria 5 e 5e funcionam igualmente na Categoria 6. Em aplicações onde são exigidas altas taxas de transmissão, os cabos Categoria 6 permitem adicionalmente a redução de custo dos equipamentos ativos utilizados na transmissão e recepção dos sinais. Por exemplo, a seguinte figura apresenta uma comparação do protocolo de transmissão Gigabit Ethernet (IEEE 1000Base-T) para sistemas baseados nos cabos de par trançado do tipo Cat5e e Cat6.

O salto de 100 Mbps para 1 Gbps (1000 Mbps) fazendo uso do cabeamento existente, ou seja, de cabos Cat-5 e e Cat-5e, está acompanhado por um número de mudanças na sinalização que tomam vantagens adicionais dessa infraestrutura já instalada na maioria das redes corporativas. Nesse sentido, para transmitir a 1 Gbps utilizando cabos Cat-5 ou Cat-5e devem ser feitas algumas modificações como explicadas a seguir.

Os cabos de par trançado do tipo Cat-5 (ou Cat-5e) são geralmente não blindados, ou seja, são do tipo UTP tendo cada um deles quatro pares internos de cabos trançados. As tecnologias FastEthernet (100Base-T) e Ethernet clássica (10Base-T) utilizam unicamente dois desses quatros pares de cabos, deixando os restantes dois pares sem uso. Já a

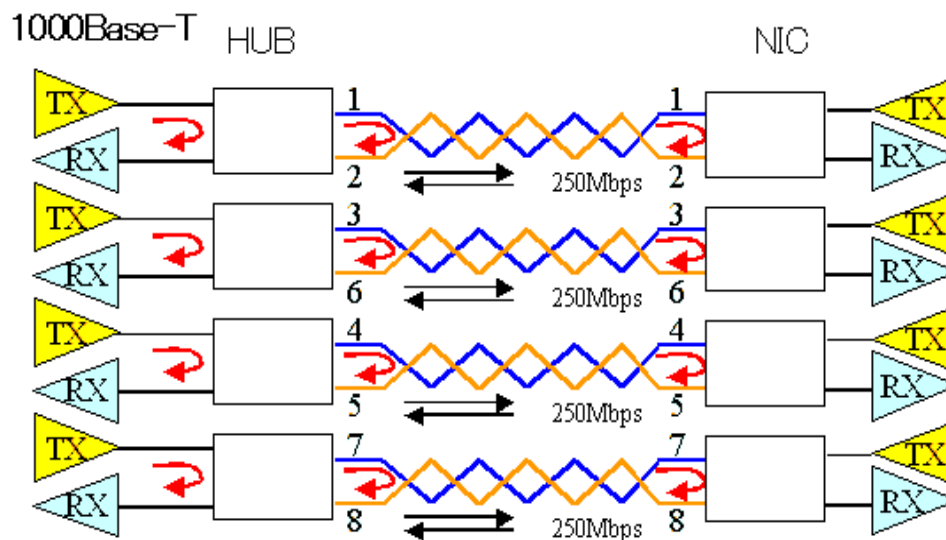
tecnologia Gigabit Ethernet (1000Base-T), que transmite a 1 Gbps, faz uso dos quatro pares de cabos.

Se fizermos uma analogia entre a tecnologia FastEthernet (100Base-T) e o modo de transferência Full-duplex observaremos que são parecidas no sentido de efetuar tanto a transmissão e recepção de dados de forma simultânea. A diferença entre a tecnologia FastEthernet (100Base-T) e a tecnologia Gigabit Ethernet (1000Base-T) é que esta última faz uso dos quatro pares para a transmissão e recepção (Tx/Rx) de dados, sendo que cada par opera a 250 Mbps. A seguir vamos estudar (em detalhe) como opera a tecnologia Gigabit Ethernet.

O Padrão IEEE Gigabit Ethernet

A tecnologia Gigabit Ethernet é um padrão que foi criado para aumentar o desempenho de redes locais baseadas nos protocolos Ethernet e FastEthernet, utilizando o mesmo formato de frame (IEEE 802.3u), os mesmos métodos de codificação e de controle de fluxo e o método CSMA/CD para o controle de acesso em redes Half-duplex.

A comunicação no padrão Gigabit Ethernet pode ser feita seguindo dois padrões:

1. O padrão IEEE 1000Base-T e
2. O padrão IEEE 1000Base-TX.

Os dois utilizam todos os 4 pares do cabo de par trançado. Nesse caso, a rede pode operar tanto no modo Full-duplex, onde os dois lados podem transmitir dados simultaneamente nos pares, quanto no modo Half-duplex, sendo dois pares para transmissão e dois para recepção. O que determina o uso de um modo ou outro são os elementos constituintes da infraestrutura da rede, isto é, o emparelhamento dos pares dentro do cabo e a eletrônica envolvida.

Padrão 1000Base-T

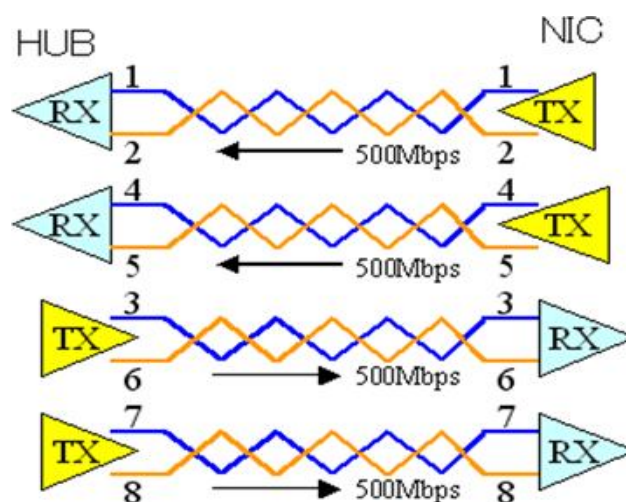
Inicialmente, a especificação 1000BASE-T foi escrita para operar sobre cabeamento UTP Cat-5. Para atingir a performance solicitada, a sinalização do padrão requer a utilização dos quatro pares trançados do cabo, utilizando um esquema de codificação PAM (Phase Amplitude Modulation) nível 5, para transmitir um espectro não filtrado de 125 MHz em canais Full-duplex, conforme a especificação da ISO/IEC 11801 e ANSI/EIA/TIA-568B. Deve-

se observar que a única diferença entre as normas TIA-568A e TIA-568B é a da troca dos pares 2 e 3 (laranja e verde).

Essa especificação (com cabos Cat-5) se destina para o cabeamento horizontal e da área de trabalho, desde que os enlaces sejam aprovados em testes adicionais de Perda de Retorno e FEXT, segundo a norma ANSI/EIA/TIA-568-B. Uma vez que no Gigabit Ethernet, cada um dos quatro pares do cabo deve suportar uma taxa efetiva de 250 Mbps em cada direção e simultaneamente, até uma distância de 100m, garantindo que a taxa de erros de bit (BER-Bit Error Rate) fique abaixo de 10^{-10}.

Para dar maior margem de segurança no atendimento aos requisitos dessa tecnologia mesmo no pior caso, ou seja, com quatro conexões (2 patch panels, 1 ponto de consolidação e 1 tomada de telecomunicação), foi elaborado o adendo conhecido como categoria 5e (Cat-5e) a letra e vem do inglês Enhanced (melhorado). Portanto, o cabeamento Cat-5e é um cabeamento do tipo Cat-5 melhorado.

Padrão 1000Base-TX

Trata-se do padrão Gigabit Ethernet sobre cabeamento UTP, só que usando uma eletrônica com aproximadamente um 75% de menor complexidade do que a eletrônica utilizada no padrão 1000Base-T.

O padrão trafega a 500 Mbps por cada par, sendo dois pares para cada sentido, ou seja, dois pares para transmissão (Tx) e dois pares para recepção (Rx).

1000Base-T vs. 1000Base-TX

Quando instalamos um cabo Cat-5e, ele trabalha na frequência até 100 MHz para a transmissão de dados, podendo alcançar 1000 Mbps utilizando quatro pares. Já os cabos Cat-6 e Cat-7[3], por exemplo, trabalham em frequências de 200/250MHz e 500/600MHz, respectivamente, para transmitir dados, alcançando os mesmos 1000 Mbps e utilizando também os mesmos quatro pares.

Para a transmissão a 1 Gbps pode-se utilizar qualquer um dos dois padrões (1000Base-T ou 1000Base-TX). Nesse caso, estará sendo definindo também o tipo de cabeamento que será utilizado, ou seja, para redes com cabeamento Cat-5e recomenda-se utilizar o padrão 1000base-T e em redes com cabeamento Cat-6 ou Cat-7, o padrão mais recomendado é o 1000base-TX. A diferença básica entre um e outro está na eletrônica envolvida, pois para uma porta 1000Base-T todos os pares devem transmitir e receber simultaneamente. Já para o padrão 1000Base-TX apenas dois pares transmitem e os outros dois pares recebem isso torna a eletrônica mais simples e barato, apesar de estarmos falando de frequências diferentes.

Resumindo, no padrão 1000BaseT, o cabeamento é mais barato (cabos Cat-5e) e o hardware envolvido é mais complexo e caro; para o padrão 1000Base-TX, o cabeamento é mais caro (cabos Cat-6 ou Cat-7) e o hardware mais barato.

Problemas De Conexão

A flexibilidade do padrão 1000Base-T possibilita uma migração relativamente simples das redes Ethernet e FastEthernet, já que é possível aproveitar a infraestrutura de cabeamento

[3]Por enquanto a Categoria 7 (Cat-7) esta em fase de testes e não é utilizada comercialmente.

existente. Como o 1000Base-T utiliza uma taxa transmissão menor por cada par, permite que o cabo seja do tipo Cat-5e. Já o 1000Base-TX exige que o cabo seja no mínimo um Cat-6.

Na verdade, pouca coisa muda na infra-estrutura. Deve-se observar apenas que, apesar dos cabos serem os mesmos (Cat-5, Cat-5e ou superior), o padrão faz uso intensivo da capacidade de transmissão e por isso detalhes como o comprimento da parte destrançada do cabo para o encaixe do conector, o nível de interferência tanto eletromagnética EMI (Electromagnetic Interference) como de radio freqüência RFI (Radio Frequency Interference) no ambiente, rotas de cabos muito longas, etc. São mais críticos para manter a performance solicitada pela rede.

As possíveis causas para uma conexão Gigabit não operar dentro da taxa efetiva de 1Gbps podem estar ligadas às condições do cabeamento existente entre os pontos de conexão, uma vez que as conexões requerem cabos e acessórios de rede instalados segundo as normas de cabeamento para redes de comunicação. Por exemplo, os Patch Cords e seus conectores também devem seguir a categoria do cabo utilizado.

Outro detalhe importante diz respeito à pinagem dos conectores. O padrão 1000Base-T utiliza quatro pares do cabo de rede, diferentemente dos padrões Ethernet clássico (10Base-T) e FastEthernet (100Base-T) que utilizam apenas dois pares. Como a sequencia das cores dos conectores do cabo é a mesma, seguindo o padrão 568A ou 568B, é importante verificar se não existem condutores defeituosos ou com mau contato nos conectores e ao longo da conexão. Esse teste de continuidade pode ser feito utilizando-se um simples multímetro na escala para medir resistores e verificar a continuidade da linha.

Resumo Do Padrão IEEE Gigabit Ethernet Com Cat-5, Cat-5e e Cat-6

Os grupos internacionais de padronização desenvolvem continuamente normas para descrever as performances necessárias dos equipamentos, cabos e demais componentes dos sistemas de cabeamento para suportar as novas tecnologias de rede que surgem. Seguindo essa linha, o padrão 1000Base-T está direcionado para proporcionar transmissões

em sistemas de cabeamento Cat-5e (por sinal, a letra **e** vem do inglês Enhanced que significa Melhorado) de ótima performance, ou performance melhorada, nos projetos de redes LAN de tamanho pequeno a médio com relativamente poucos serviços.

O cabeamento do tipo Cat-6 deve ser utilizado para redes novas e de maior porte (neste caso utilizar o padrão 1000Base-TX). Assim, os novos projetos de infraestrutura baseados no padrão Gigabit Ethernet devem ser executados utilizando preferencialmente os elementos de cabeamento de categoria superior disponíveis para garantir uma escalabilidade e vida útil mais longa para a infraestrutura. Para rodar aplicações Gigabit Ethernet em redes utilizando cabeamento Cat-5, os equipamentos eletrônicos (Hubs, Switches, etc.) devem oferecer recursos para compensar a degradação do sinal no canal (o que pode elevar seu custo). Tecnologias que usam adaptadores de filtragem digital também são utilizadas para cancelar o NEXT e o eco nestes sistemas. Após a instalação dos cabos e conectores, deve ser executada a certificação através de equipamentos de testes, adequados às características do sistema.

UNIDADE 10

Objetivo: Ter uma noção básica porem completa sobre as fibras ópticas.

Cabeamento De Redes (Parte II)

Fibras Ópticas

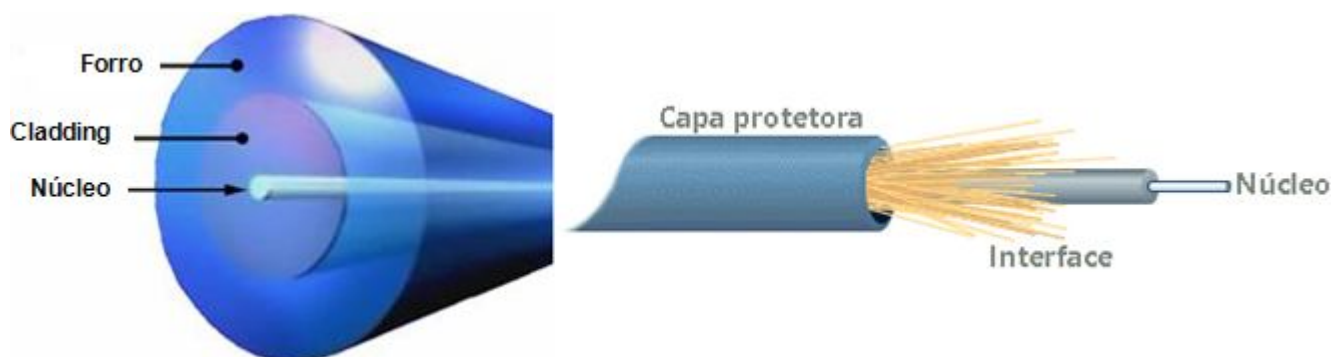
Sem as fibras ópticas, a Internet e até o sistema telefônico que temos atualmente teriam sido quase que inviáveis. Com a migração das tecnologias de rede para padrões de maiores velocidades como nas redes FDDI (Fiber Distributed Digital Interface), ATM, FastEthernet, GigaEthernet, 10GigaEthernet, 100FastEthernet, etc. o uso de fibras ópticas foi ganhando força também nas redes locais do tipo LAN.

O produto começou a ser fabricado em 1978 e passou a substituir os cabos coaxiais nos Estados Unidos na segunda metade dos anos 80. Em 1988, o primeiro cabo submarino de fibras ópticas mergulhou no oceano, dando início à superestrada da informação. O físico indiano Narinder Singh Kanpany é o inventor da fibra óptica, que passou a ter aplicações práticas na década de 60 com o advento da criação de fontes de luz de estado sólido, como o raio laser e o diodo emissor de luz LED (Light Emitter Diode).

Existem dois tipos de fibras ópticas: As fibras multímodo e as monomodo. A escolha de um desses tipos dependerá da aplicação da fibra. As fibras multímodo são mais utilizadas em aplicações de rede locais (LAN), enquanto as monomodo são mais utilizadas para aplicações de rede de longa distância (WAN), estas últimas são mais caras, porém muito mais eficientes que as fibras multímodo. Aqui no Brasil, a utilização mais ampla da fibra óptica teve início na segunda metade dos anos 90, impulsionada pela implementação dos Backbones das operadoras de redes metropolitanas.

Ao contrário dos cabos coaxiais e de par trançado, que nada mais são do que fios de cobre que transportam sinais elétricos, a fibra óptica transmite luz e por isso é totalmente imune a

qualquer tipo de interferência eletromagnética. Além disso, como os cabos são feitos de plástico e fibra de vidro (ao invés de metal), são resistentes à corrosão.

O cabo de fibra óptica é formado por um núcleo extremamente fino de vidro, ou mesmo de um tipo especial de plástico. Uma nova cobertura de fibra de vidro, bem mais grossa envolve e protege o núcleo. Em seguida temos uma camada de plástico protetora chamada de Cladding (revestimento), uma nova camada de isolamento e finalmente uma capa externa chamada bainha.

A transmissão de dados por fibra óptica é realizada pelo envio de um sinal de luz codificado, dentro do domínio de frequência do infravermelho a uma velocidade de 10 a 15 MHz. O cabo óptico consiste de um filamento de sílica e de plástico, onde é feita a transmissão da luz.

As fontes de transmissão de luz podem ser diodos emissores de luz (LED) ou lasers semicondutores. O cabo óptico com transmissão de raio laser é o mais eficiente em potência devido a sua espessura reduzida. Já os cabos com diodos emissores de luz são muito baratos, além de serem mais adaptáveis à temperatura ambiente e de terem um ciclo de vida maior que o do laser.

O cabo de fibra óptica pode ser utilizado tanto em ligações ponto-a-ponto (fibras monomodo) quanto em ligações multiponto (fibras multímodo). As fibras multímodo permitem a transmissão de muitos canais de informação de forma simultânea pela mesma fibra. Isto é possível através da técnica de multiplexação por divisão da longitude de onda (λ), onde cada sinal luminoso é transmitido num comprimento ou longitude de onda diferente.

As partes condutoras de luz de uma fibra óptica são chamadas de núcleo e revestimento. O núcleo é geralmente um vidro muito puro com um alto índice de refração. Quando o vidro do núcleo é envolto por uma camada de vidro ou de plástico com baixo índice de refração, a luz pode ser mantida no núcleo da fibra. Esse processo é chamado de reflexão interna total e permite que a fibra óptica atue como um duto de luz conduzindo a luz por distâncias enormes, até mesmo em curvas.

O custo do metro de cabo de fibra óptica não é elevado em comparação com os cabos convencionais. Entretanto seus conectores são bastante caros, assim como a mão de obra necessária para a sua montagem. A montagem desses conectores, além de um curso de especialização, requer instrumentos especiais, como microscópios, ferramentas especiais para corte e polimento, medidores e outros aparelhos sofisticados.

Devido ao seu elevado custo, os cabos de fibras ópticas são usados apenas quando é necessário atingir grandes distâncias em redes que permitem segmentos de até 1 Km, enquanto alguns tipos de cabos especiais podem conservar o sinal por até 10 Km (distâncias maiores são obtidas usando repetidores).

Mesmo permitindo distâncias tão grandes, os cabos de fibra óptica permitem taxas de transferências de até 155 Mbps, sendo especialmente úteis em ambientes que demandam uma grande transferência de dados. Como não soltam faíscas, os cabos de fibra óptica são mais seguros em ambientes onde existe perigo de incêndio ou explosões.

E para completar, o sinal transmitido através dos cabos de fibra é mais difícil de interceptar, sendo os cabos mais seguros para transmissões sigilosas.

A seguir os padrões mais comuns de redes usando fibra óptica:

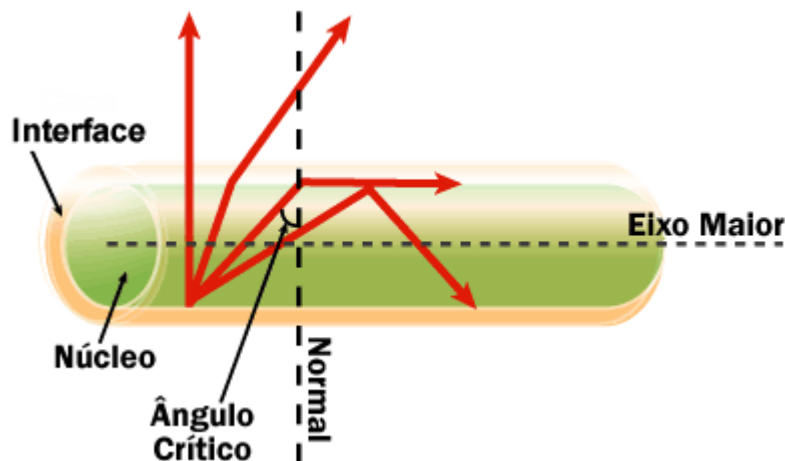
- FDDI (Fiber Distributed Data Interface)
- FOIRL (Fiber – Optic InterRepeater Link)
- 10BaseFL
- 100BaseFX
- 1000BaseSX
- 1000BaseLX

Princípio De Funcionamento Das Fibras Ópticas

O princípio pelo qual a luz se propaga no interior da fibra é fundamentado na reflexão total da luz vejamos o porquê disto. Quando um raio de luz se propaga em um meio cujo índice de reflexão é n_1 (do Núcleo) e atinge a superfície de outro meio com índice de refração n_2 (do revestimento ou Cladding), onde $n_1 > n_2$ e, desde que o ângulo de incidência (em relação à normal) seja maior ou igual ao ângulo crítico, ocorrerá o fenômeno de reflexão total. Portanto, o resultado disso é o retorno do raio de luz ao meio com maior índice de refração n_1, ou seja, a luz continuará sua viagem pelo núcleo.

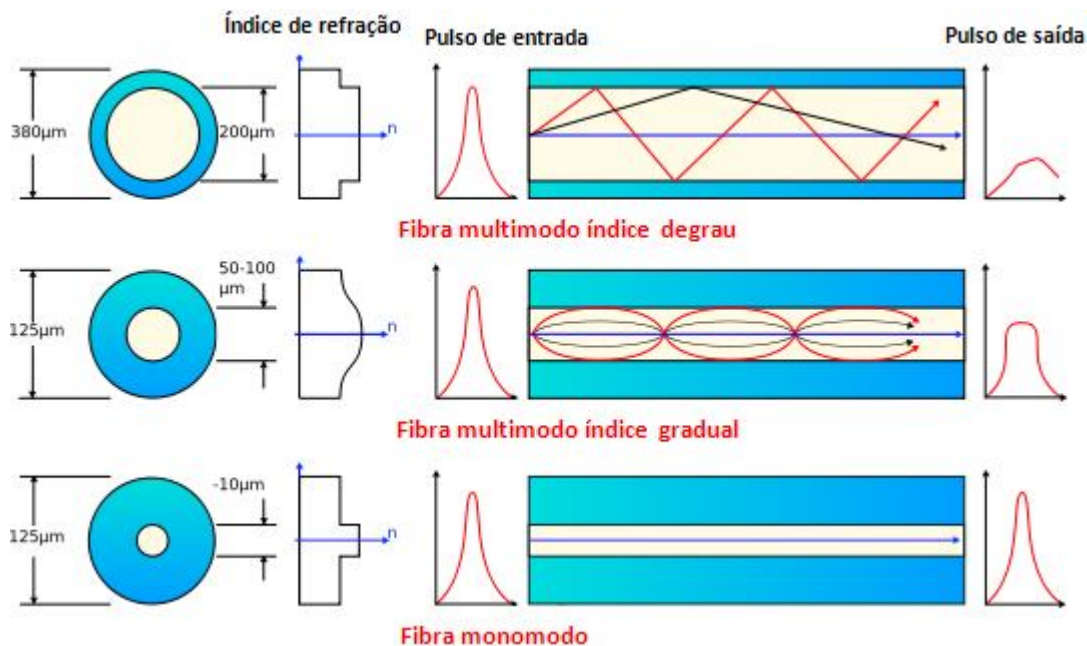
Em física, o ângulo crítico é descrito em relação à linha normal. Para as fibras ópticas, o ângulo crítico é descrito em relação ao eixo paralelo que corre pelo meio da fibra. Assim, o ângulo crítico da fibra óptica é igual a 90 graus menos o ângulo crítico (ou ângulo limite).

Em uma fibra óptica, a luz viaja através do núcleo, porque o ângulo de incidência do feixe de luz é sempre maior do que o ângulo crítico. A luz se refletirá na interface, não importando o

ângulo em que a fibra seja curvada, mesmo que seja um círculo completo. Como a interface não absorve nenhuma luz do núcleo, a onda luminosa pode viajar grandes distâncias.

Baseado neste princípio, a luz é injetada em uma das extremidades da fibra óptica sob um cone de aceitação, onde este determina o ângulo pelo qual o feixe de luz deverá ser injetado para que o mesmo possa se propagar ao longo da fibra óptica.

As fibras são constituídas, basicamente, de materiais dielétricos possuindo uma estrutura cilíndrica, composta de uma região central, denominada núcleo, por onde trafega a luz, e uma região periférica, denominada casca que envolve completamente o núcleo.

As dimensões variam conforme os tipos de fibras ópticas onde o núcleo pode varias de 8 µm (micrometros) até 200 µm e a casca de 125 µm até 380 µm, contudo dentre as fibras ópticas mais utilizadas no mercado atualmente, as dimensões mais utilizadas são de 8 e 62,5 µm para o núcleo e 125 µm para a casca. As fibras ópticas de outras dimensões foram bastante utilizadas no passado, por uma questão de padronização de mercado, estas dimensões caíram em desuso.

Nota: 1 µm (micrometro) = 10^{-6} metros, 1 nm (nanômetro) = 10^{-9} metros

Características (segundo o material de construção) das Fibras Ópticas:

- Vidro (Sílica):
    - Fibras monomodo índice degrau
    - Multímodo índice gradual
    - Multímodo índice degrau
- Sílica com casca plástica (PCS): Fibras de índice degrau
- Somente casca plástica: Fibras de índice degrau

Fibras Monomodo Índice Degrau

A fibra monomodo de índice degrau vai um passo à frente. O tamanho do núcleo, 8 µm de diâmetro, e a relação de índices entre o núcleo e o Cladding permite que apenas um modo seja propagado através da fibra, consequentemente diminuindo a dispersão do pulso

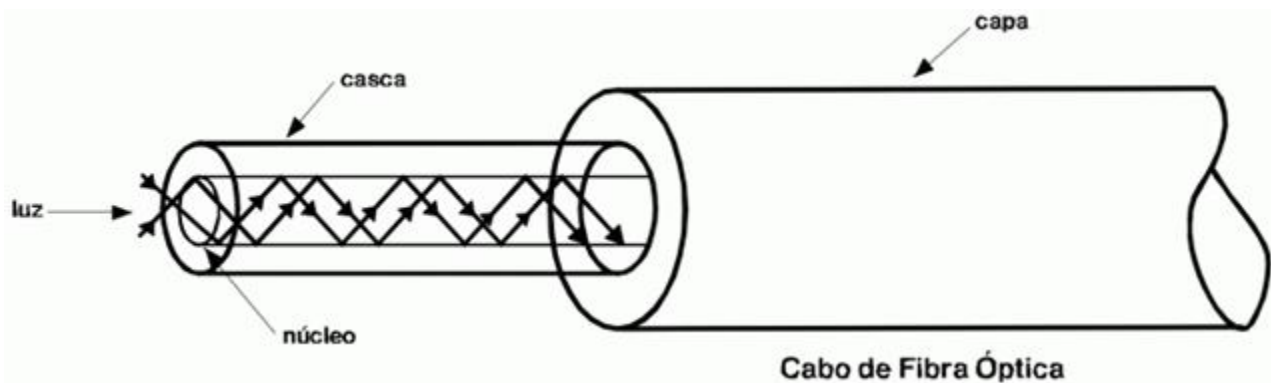
luminoso. A emissão de sinais monomodo só é possível com laser, podendo atingir taxas de transmissão na ordem de 100 GHz/Km, com atenuação entre 0,2 dB/Km e 0,7 dB/Km. Contudo, o equipamento como um todo é mais caro que o dos sistemas multimodo. Essa fibra possui uma grande expressão em sistemas telefônicos.

Algumas das características deste tipo de fibras ópticas são:

- Aplicações para grande largura de banda 350 GHz (1991)
- Baixas perdas: tipicamente 0,2-0,3 dB/Km até 0,5-0,7 dB/Km com um comprimento de onda de 1300 nm (nanômetros), e 0,2 dB/Km com comprimento de onda de 1550 nm.
- Área do diâmetro do Campo modal de 10 μm
- Diâmetro Externo de Revestimento de 125 μm
- Custos superiores para conectores, emendas, equipamentos de teste e transmissores/ receptores.
- Transmite um modo ou caminho de luz.
- Transmite em comprimento de onda de 1300 e 1550 nm
- Fabricada em comprimento de até 25 Km
- Sensível a dobras (curvaturas).

Fibras Multímodo Índice Gradual

A fibra óptica multimodo de índice gradual (Grated Index), constitui uma evolução da fibra óptica multímodo índice degrau, projetada para prover uma melhor propagação dos feixes de luz incidentes na fibra óptica multimodo. Neste tipo de fibra óptica viajam vários feixes ópticos simultaneamente. Estes feixes são refletidos com diferentes ângulos nas paredes do núcleo, isto permite que eles percorram diferentes distâncias, y se dissipem no trajeto dentro da fibra, razão pela qual a distância de transmissão é curta.

Cabo de Fibra Óptica

Existe um limite para o ângulo de incidência do feixe luminoso dentro da fibra óptica, si este limite é ultrapassado o feixe de luz não se reflete mais e irá se refratar, consequentemente não continuará o percurso desejado.

As características mais importantes deste tipo de fibras ópticas são:

- Largura de Banda da ordem de1500 MHz - Km
- Perdas de 1 a 6 dB/Km
- Núcleos de 50/ 62/ 85/ 100 µm (Padrões CCITT)
- Diâmetro Externo do Revestimento de 125 e 140 µm
- É eficaz com fontes de laser e LED
- Componentes equipamentos de teste e transmissores/ receptores de baixo custo.
- Transmite muitos modos (aproximadamente 500) ou caminhos de luz, admite muitos modos de propagação.
- Possui limitação de distância devido às altas perdas e dispersão modal.
- Transmite a 820-850 e 1300 nm.
- Fabricadas em comprimentos até 2,2 Km

Vantagens Das Fibras Ópticas

- **Imunidade a Interferências**: O feixe de luz transmitido pela fibra óptica não sofre interferência de sistemas eletromagnéticos externos.
- **Sigilo**: Devido a dificuldades de extração do sinal transmitido, obtém-se sigilo nas comunicações.
- **Tamanho Pequeno**: Um cabo de 3/8 de polegada (9,18mm) com 12 pares de fibra, operando a 140 MBPS pode carregar tantos canais de voz quanto um de 3 polegadas (73mm) de cobre com 900 pares trançados. Menor tamanho significa melhor utilização de dutos internos.
- **Condutividade elétrica nula**: A fibra óptica não precisa ser protegida de descargas elétricas, nem mesmo precisa ser aterrada, podendo suportar elevadas diferenças de potencial.
- **Leveza**: O mesmo cabo óptico citado no item 2 pesa aproximadamente 58 kg/km. O cabo de pares trançados pesa 7.250 Kg/km. Isto possibilita maiores lances de puxamento para o cabo de fibra óptica.
- **Largura de Banda**: Fibras ópticas foram testadas até os 350 bilhões de bits por segundo em uma distância de 100 km. Taxas teóricas de 200-500 trilhões de bits por segundo são alcançáveis.
- **Baixa Perda**: As fibras monomodo atuais possuem perdas tão baixas quanto 0,2 dB/km (com um comprimento de onda de 1550 nm).
- **Imunidade a Ruídos**: Diferente dos sistemas metálicos, que requerem blindagem para evitar radiação e captação eletromagnética, o cabo óptico é um dielétrico e não é afetado por interferências de radiofrequência ou eletromagnéticas. As fibras ópticas são o único meio que podem transmitir através de ambientes sob severa radiação.

- **Integridade de Dados**: O potencial para baixas taxas de erro de bit eleva a eficiência do circuito. Em condições normais de funcionamento a fibra óptica apresenta uma taxa de erro de bit (Bit Error Rate) BER de 10^{-11}, ou seja, que de mais de 100 mil milhões de bits enviados um estaria com erro. Esta característica permite que os protocolos de alto nível, para correção de erros, não sejam muito (ou quase nada) utilizados.

- **Alta Faixa de Temperatura**: Fibras e cabos podem ser fabricados para operar em temperaturas de -40º C até 93ºC. Há registros de resistência à temperatura de -73ºC até 535ºC.

- **Sem Risco de Fogo ou Centelhamento**: As fibras ópticas oferecem um meio para dados sem circulação de corrente elétrica. Para aplicações em ambientes perigosos ou explosivos a fibra óptica representa uma forma de transmissão segura.

- **Durabilidade**: A fibra óptica é resistente à corrosão e às altas temperaturas, e graças à proteção da envoltura é capaz de suportar esforços elevados de tensão na instalação o que garante uma boa durabilidade do cabo.

Desvantagens das Fibras Ópticas

- Fragilidade (curvas em dutos podem quebrar a fibra)

- De difícil conexão (é necessária a utilização de microscópios)

- Dificuldade de utilização em topologias físicas de barramento.

Tipos De Emendas

Basicamente temos dois tipos de emendas utilizados na junção de cabos de fibra ópticos:

1. **Emenda Mecânica:** Este tipo de emenda é muito utilizado nos Estados Unidos, pela AT&T. No Brasil, encontra muita aplicação no reparo emergencial de cabos ópticos. Consiste na utilização de conectores mecânicos, com a utilização de cola e polimento. Alguns tipos não se baseiam no polimento, devendo neste caso as fibras serem muito bem clivadas.

2. **Emenda por Fusão**: Este tipo de emenda é a das mais importantes e a mais utilizada atualmente. As duas extremidades a serem unidas são aquecidas até o ponto de fusão, enquanto uma pressão axial adequada é aplicada no sentido de unir as partes. Importante deixar ambas as extremidades separadas por uma distância de 10 a 15um, para permitir a dilatação do vidro.

Para proteger a emenda por fusão é utilizado o protetor de emenda, que deve prover proteção mecânica e contra a penetração de umidade o protetor de emenda é composto por três elementos básicos:

- Tubo externo Termocontrátil,
- Tubo interno,
- Elemento de sustentação mecânica.

Para se fazer uma boa emenda é fundamental uma boa clivagem e limpeza da fibra, além do bom ajuste da máquina de emenda.

Os conectores ópticos, como o próprio nome diz, têm a função de conectar a fibra óptica ao componente ópticos dos equipamentos, ou seja, Emissor de Luz (LASER ou LED) e Fotodetector. É um componente de extrema importância na rede, sendo que mal utilizado pode comprometer a confiabilidade do sistema. Os conectores ópticos utilizados nos sistemas de Telecomunicações são montados em laboratórios apropriados, devendo ser avaliados com relação à sua perda por inserção (dB).

O processo de montagem de um conector consiste de:

- Preparação do cabo;
- Montagem do conector;
- Cura da resina;
- Polimento;
- Testes ópticos.

Fatores que causam atenuação alta no conector, com relação á qualidade da face:

- Excesso de cola no núcleo do conector;
- Fibra quebrada ou trincada;
- Riscos na face do conector;
- Falta de polimento p/ remover impurezas na face;
- Sujeira.

Material Da Fibra Óptica

Existem basicamente três tipos de cabos:

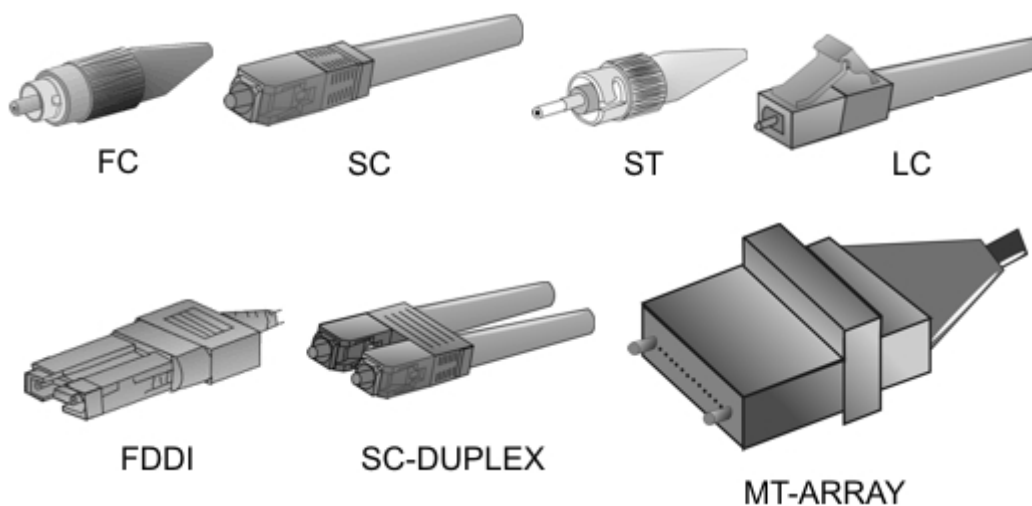
- **Sílica/Sílica**: O núcleo e a casa são de vidro de sílica Neste caso há fibras ópticas monomodo, índice degrau e gradual e fibras ópticas multimodo, índice degrau e gradual. São fibras ópticas de alto desempenho e tamanhos reduzidos.
- **Plástico**: O núcleo e a casca são de plástico (polímero). São essencialmente fibras ópticas multimodo e operam na faixa de 620 a 700 nm. Possui diâmetros maiores, menor capacidade, baixa velocidade e alcance de transmissão reduzida.

- **Sílica/Plástica**: O núcleo é de sílica e a casca de plástico. Possuem um desempenho intermediário entre as fibras de sílica/sílica e a de plástico.

Dimensões da Fibra

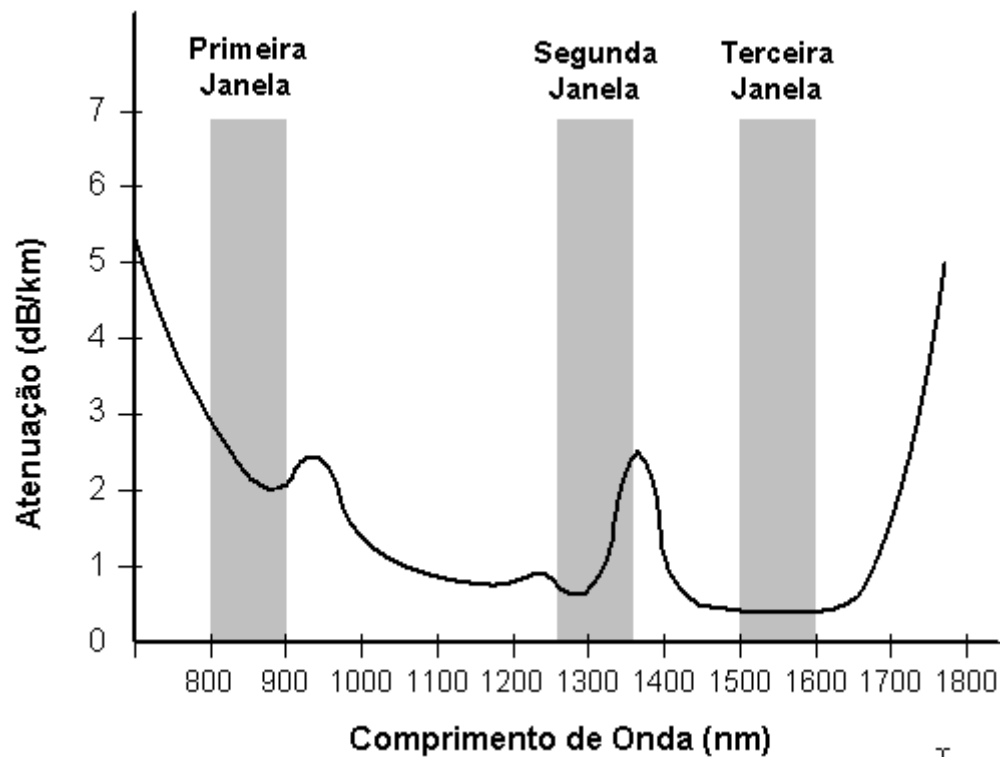
	Sílica/Sílica monomodo	**Sílica/Plástica multimodo**	**Fibra óptica Plástica**	**Fio de cabelo**
Diâmetro da casca	125 µm	125 µm	500/1000 µm	75 µm
Diâmetro do núcleo	18/10 µm	50/62,5 µm	125/980 µm	

Principais Tipos de Conectores

- **Quanto à Tecnologia**: FC, LC, SC, ST, SMA, BICÔNICO, E2000, FDDI, SC-Duplex, MT-Array, etc.
- **Quanto ao Polimento**: PC, SPC, UPC, APC.
- **Quanto ao material do ferrolho**: Cerâmica, AÇO, INOX.

Usando fibra óptica de sílica e sistema multimodo, sem modulação, a distância de transmissão de vídeo analógico pode chegar a até 5 km dependendo da tecnologia. Usando sistema monomodo, o alcance é estendido para até 25 km podendo chegar a 50 km se usar elementos especiais.

Janelas Ópticas

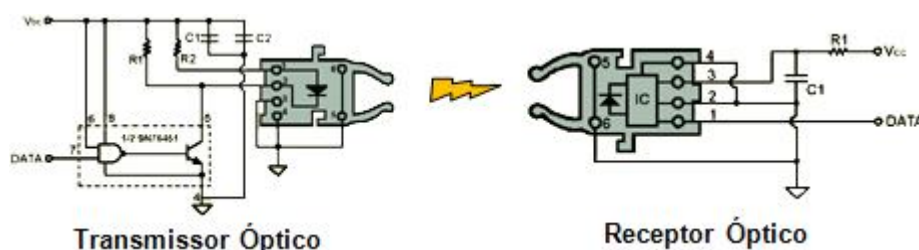
As janelas ópticas de transmissão dizem respeito às regiões de comprimento de onda aonde a atenuação óptica é baixa e pode ser utilizada. Estas janelas ópticas estão relacionadas às faixas de frequência utilizadas para transmissão de sinais luminosos por fibras ópticas, regiões espectrais de atenuação mínimas em torno dos seguintes comprimentos de onda de λ = 850 nm, λ = 1300 nm e λ = 1550 nm são úteis para transmitir informação com perdas (por atenuação) mínimas.

Janela Óptica	**Largura da Janela Óptica**	**Comprimento de Onda (λ) de Operação**	**Atenuação (aproximada)**
Primeira	De λ = 800 a 900 nm	λ = 850 nm	~ 20 dB/km
Segunda	De λ = 1260 a 1360	λ = 1310 nm	~ 0,3 a 0,5 dB/km
Terceira	De λ = 1500 a 1600 nm	λ = 1550 nm	~ 0,18 a 0,25 dB/km

A figura anterior mostra a curva relativa à atenuação em função do comprimento de onda (λ) das três janelas de transmissão de uma fibra óptica.

Transmissor Óptico

É utilizado um diodo laser (LD) ou diodo emissor de luz (LED) para converter os sinais elétricos em sinal luminoso. Como indica a curva relativa à atenuação-comprimento de onda assim como a informação dada das janelas de transmissão de uma fibra óptica, os feixes luminosos no infravermelho com comprimento de onda de λ = 850 nm, λ = 1.310 nm e λ = 1.550 nm são os mais utilizados. Assim, os dispositivos comumente utilizados como fonte de luz, nos transmissores ópticos, operam na faixa do infravermelho (de 750nm a 1mm) do espectro eletromagnético e, por isso, a sua luz de saída é normalmente invisível aos olhos humanos.

Receptor Óptico

O receptor óptico está composto de um dispositivo fotoelétrico e de um estágio eletrônico de amplificação e filtragem. O dispositivo fotoelétrico é responsável pela detecção e conversão do sinal luminoso em sinal elétrico. Para transmitir informação (sinal elétrico) através de uma fibra óptica, a mesma deve ser primeiramente convertida em um sinal óptico e depois reconvertida no receptor. Na prática, o sinal óptico atenua-se durante a transmissão através da fibra. A atenuação depende do comprimento de onda do feixe de luz (como apresentado na tabela anterior).

Quadro Comparativo dos Meios de Transmissão por Cabo

Características/ Meio	**Par Trançado**	**Cabo Coaxial "Base Band"**	**Cabo Coaxial "Broadband"**	**Fibra Óptica**
Tipo de Sinalização	Digital e analógica	Digital	Analógica	Transmissão de luz
Disponibilidade de Componentes	Alta disponibilidade	Limitada	Alta disponibilidade	Limitada
Custo de Componente	Mais baixo de todos	Baixo	Médio	Alto
Complexidade de Interconexão	Mais baixo de todos	Baixa	Média	Alta

Facilidades para Ligação Multiponto	Baixa	Média (100s nós)	Alta (1000s nós)	Muito Baixa
Topologias Adequadas	Todas	Todas	Barra	Estrela e Anel
Números de Nós (típico em ligação multiponto)	10s	10s a 100s	100s/canal	2 (ponto a ponto)
Relação Sinal/Ruído	Baixa	Média	Média	Alta

Padrão 10GigaEthernet

A partir do ano de 2004, a família do padrão 10GigaEthernet (IEEE 802.3ae), que faz uso de forma exclusiva das fibras ópticas como meio de transmissão e de acordo com a janela óptica em questão, esta composta da seguinte maneira:

Utilizando a 1ª janela óptica:

- **10GBase-SR**: 10Gb sobre fibra óptica multimodo com emissores de 850 nm, com um alcance máximo de 26 a 82 metros. Com emissores laser otimizados pode alcançar os 300 metros. Formato do quadro para redes LAN.
- **10GBase-SW**: 10Gb sobre fibra óptica multimodo com emissores de 850 nm, com um alcance máximo de 26 a 82 metros. Com emissores laser otimizados pode alcançar os 300 metros. Formato do quadro para redes WAN, compatível com redes SONET.

Utilizando a 2ª janela óptica:

- **10GBase-LR**: 10Gb sobre fibra óptica monomodo com emissores de 1300 nm, com um alcance máximo de 10 Km. Formato do quadro para redes LAN.

- **10GBase-LW**: 10Gb sobre fibra óptica monomodo com emissores de 1300 nm, com um alcance máximo de 10 Km. Formato do quadro para redes WAN, compatível com redes SONET.
- **10GBase-LX4**: Utiliza quatro emissores laser e quatro receptores na ordem dos 1300 nm, com um alcance máximo de 300 metros sobre fibra multimodo, e de 10 Km. sobre fibra monomodo. Formato do quadro apto para redes LAN.

Utilizando a 3ª janela óptica:

- **10GBase-ER**: 10Gb sobre fibra óptica monomodo com emissores de 1550 nm, com um alcance máximo de 40 Km. Formato do quadro para redes LAN.
- **10GBase-EW**: 10Gb sobre fibra óptica monomodo com emissores de 1550 nm, com um alcance máximo de 40 km. Formato do quadro para redes WAN, compatível com redes SONET.

Atividades

Antes de dar continuidades aos seus estudos é fundamental que você acesse sua SALA DE AULA e faça a Atividade 1 no “link” ATIVIDADES.

UNIDADE 11

Objetivo: Entender quais os padrões existentes atualmente para redes.

Padrões para Meios de Redes

Ao projetar e criar redes, é necessário certificar-se de que todos os códigos contra incêndio, os códigos da construção civil e os padrões de segurança aplicáveis sejam obedecidos. Devem-se também seguir todos os padrões de desempenho estabelecidos para garantir uma ótima operação da rede e, devido à grande variedade de opções disponíveis nos meios de rede, garantir a compatibilidade e a interoperabilidade.

Padrões para meios de rede desenvolvidos e publicados pelos grupos:

- IEEE - Institute of Electrical and Electronics Engineers;
- UL - Underwriters Laboratories (padrões de segurança);
- EIA - Electrical Industries Association;
- TIA - Telecommunications Industry Association.

A EIA e a TIA publicaram em conjunto uma lista de padrões frequentemente listados como padrões TIA/EIA. De todas as organizações a TIA/EIA foi a que teve o maior impacto nos padrões dos meios de rede. Especificamente, o TIA/EIA-568-A e o TIA/EIA-569-A foram e continuam a ser os padrões de desempenho técnico dos meios de rede mais amplamente usados. O padrão TIA/EIA-568-A especifica cinco categorias, sendo elas o cabeamento Categoria 1 (Cat 1), o de Categoria 2 (Cat 2), a Categoria 3 (Cat 3), a Categoria 4 (Cat 4) e Categoria 5 (Cat 5). Dessas, apenas a Cat 3, Cat 4 e Cat 5 são reconhecidas para uso em redes LAN. Dessas três categorias, a Cat 5 é freqüentemente recomendada e implementada nas instalações atuais de rede.

Os meios de rede que são reconhecidos para essas 5 categorias são:

- Par trançado blindado;
- Par trançado não blindado;
- Cabo de fibra óptica;
- Cabo coaxial.

Para o cabo de par trançado blindado, o padrão TIA/EIA-568-A requer cabo de 150 Ohms de dois pares. Para o par trançado não blindado, o padrão requer um cabo de 100 Ohms de quatro pares. Para fibra óptica, o padrão requer um cabo multímodo de 62.5/125 de duas fibras. Embora o cabo coaxial de 50 Ohms seja um tipo reconhecido de meio de rede no TIA/EIA-568-A, ele não é recomendado para novas instalações. Além disso, esse tipo de cabo coaxial deve ser retirado da lista de meios de rede reconhecidos na próxima vez que o padrão for revisto.

Distâncias

De acordo com o TIA/EIA-568-A, a distância máxima para lances de cabo em cabeamento horizontal é de 90 metros. Isso vale para todos os tipos de meios de redes reconhecidos CAT 5 UTP. O padrão também especifica que *jumpers* de conexão horizontal não podem ultrapassar seis metros de comprimento. O TIA/EIA-568-A também permite três metros para os *patch cables* que são usados para conectar equipamentos na área de trabalho. Os comprimentos totais dos *patch cables* e dos *jumpers* de conexão horizontal usados no cabeamento (valha a redundância) horizontal não podem ultrapassar dez metros. Os padrões mais recentes da indústria desenvolvidos para o cabeamento estruturado são as categorias Cat 5e (*enhanced* – melhorado), Cat 6, Cat 6a (*advanced* - avançado) e Cat 7, que oferecem aperfeiçoamentos superiores ao Cat 5.

A tabela mostra uma visão geral das normas EIA/TIA adotadas no cabeamento estruturado.

Norma	Assunto
EIA/TIA 568	Especificação geral sobre cabeamento estruturado em instalações comerciais.
EIA/TIA 569	Especificações gerais para encaminhamento de cabos (Infraestrutura, canaletas, bandejas, eletrodutos, calhas).
EIA/TIA 606	Administração da documentação.
EIA/TIA 607	Especificação de aterramento.
EIA/TIA 570	Especificação geral sobre cabeamento estruturado em instalações residenciais.

A Hierarquia Ethernet

Tipo	Meio	Largura de Banda Máxima	Tamanho Máximo de Segmento	Topologia Física	Topologia Lógica
10Base5	Coaxial Grosso	10 Mbps	500 m.	Barramento	Barramento
10BaseT	UTP Cat. 5	10 Mbps	100 m.	Estrela[4]	Barramento
10BaseFL	Fibra óptica Multímodo	10 Mbps	2000 m.	Estrela	Barramento
100BaseTX	UTP Cat. 5	100 Mbps	100 m.	Estrela	Barramento
100BaseFX	Fibra óptica Multímodo	100 Mbps	2000 m.	Estrela	Barramento
1000BaseT	UTP Cat. 5	1000 Mbps	100 m.	Estrela	Barramento

[4] Também pode ser Estrela estendida.

UNIDADE 12

Objetivo: Entender como os protocolos facilitam a comunicação das máquinas.

Protocolos de Redes

Um protocolo de comunicação é um conjunto de regras e convenções precisamente definidas que permitem a comunicação através de uma rede. Esse conjunto de regras estabelece como um computador conecta-se ao outro, como se identifica, quando pode enviar ou receber informações e quanto tempo pode esperar para que cada evento ocorra, bem como a forma de se desfazer a conexão.

Os dados trocados por determinado protocolo são denominados PDU's (Protocol Data Units). Por exemplo: Os PDU's do protocolo IP são chamados de datagramas ou simplesmente pacotes IP.

Além de estabelecer comportamentos para as situações normais de funcionamento de uma rede, um protocolo deve também possuir regras para as situações anormais, especificando como normalizar tais situações.

Dois ou mais computadores que desejarem trocar informações entre si, deverão seguir os mesmos protocolos. Os protocolos devem ser compatíveis nos meios digitais de forma que as transferências de informações sejam corretas.

Basicamente os protocolos são a parte do sistema operacional da rede encarregada de ditar as normas e regras para a comunicação entre os dispositivos em questão. Os mais utilizados são:

- **TCP/IP**: Transmission Control Protocol/Internet Protocol. Foi desenvolvido para ser um protocolo roteável, e serve como padrão para redes de longa distância (WAN) e para acesso a Internet.

- **IPX/SPX**: Internet Packet Exchange/Sequence Packet Exchange. Foi desenvolvido para suportar redes NetWare/Novell, redes de tamanho pequeno e médio e também tem a capacidade básica de roteamento.

- **NetBEUI**: Network Basic End User Interface. Suporta pequenas LANs é rápido e simples. Não é utilizado na Internet, apenas em redes pequenas, pois tem uma estrutura arquitetônica inerente que limita sua eficiência à medida que a rede se expande.

- **FTP**: File Transfer Protocol ou Protocolo de transferência de arquivos oferece um meio de transferência e compartilhamento de arquivos remotos. Entre os seus serviços, o mais comum é o FTP anônimo, pois permite o Download de arquivos contidos em diretórios sem a necessidade de autenticação.

- **WAP**: Wireless Application Protocol ou Protocolo de Aplicação sem-fio é um protocolo desenvolvido para ambientes móveis que necessitem de informações independentemente de sua localidade física. Ele é um padrão desenvolvido por grandes empresas de telefonia móvel para ser usado de forma que aparelhos como celulares ou "palms" sejam capazes de acessar informações disponíveis na Internet. Com o WAP é possível acessar informações sobre contas bancárias, ler e até mesmo enviar e-mails, consultar a programação da TV e realizar qualquer outra tarefa que esteja disponível na Internet para a tecnologia WAP através da mobilidade criada pelo uso de aparelhos celulares.

UNIDADE 13

Objetivo: Entender o que significa e qual a importância do modelo OSI.

O Modelo OSI

A Organização Internacional para a Padronização (International Standard Organization – ISO) é a instituição responsável pela implantação de um modelo geral e uniforme para interconexão de sistemas, denominado Modelo de Referência para a Interconexão de Sistemas Abertos, ou de forma simplificada, o modelo OSI.

O objetivo principal do modelo OSI é proporcionar uma base para a coordenação do desenvolvimento de padrões relativos à interconexão de sistemas de maneira flexível e utilizando facilidades de comunicação de dados.

Conceitos e Objetivos

O modelo OSI diz respeito à interconexão de sistemas - o modo como eles trocam informações - e não às funções internas que são executadas por um dado sistema. O modelo OSI oferece uma visão generalizada de uma arquitetura estratificada e organizada em camadas. Pela definição que foi dada a sistema, a arquitetura aplica-se a sistemas muito simples, como a conexão de um terminal a um computador, e a sistemas muito complexos, como a interconexão de duas redes completas de computadores. OSI também pode ser usado como modelo para uma arquitetura de rede. O desenvolvimento deste modelo está constantemente sofrendo alterações para poder adaptar-se aos diversos sistemas existentes.

Modelo por Camadas

O modelo OSI utiliza uma abordagem estratificada com certos conjuntos de funções alocados nas diferentes camadas que o compõem.

Uma entidade é um elemento ativo em uma camada. Duas entidades em uma mesma camada são denominadas entidades pares. As entidades de uma camada prestam serviços às entidades da camada imediatamente acima e, por sua vez, recebem serviços da camada situada imediatamente abaixo. Por exemplo, as entidades da camada de apresentação prestam serviços à camada de aplicação e recebem serviços da camada de sessão. Nesse sentido temos:

- **Física:** Ativação e desativação das conexões físicas, mediante solicitação da camada de enlace de dados. Transmissão dos bits por uma conexão física em modo síncrono ou assíncrono. Tratamento das atividades de gerência da camada física, inclusive a ativação e o controle de erros.

- **Enlace de Dados:** Estabelecimento e liberação de conexões de enlace de dados. Sincronização da recepção de dados que tiverem sido partidos por várias conexões físicas. Detecção e correção de erros de transmissão, com retransmissão de quadros, se necessário.

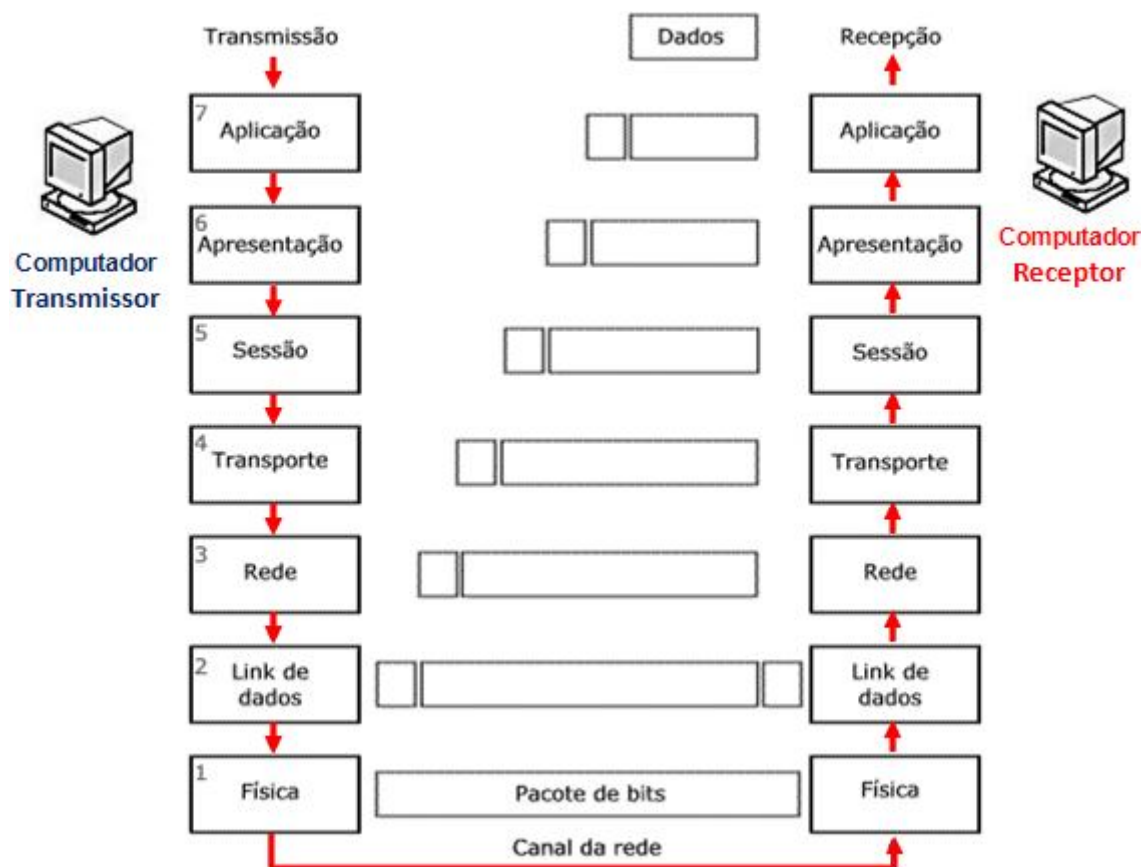
- **Rede:** Determinação de um roteamento ótimo sobre as conexões de rede que podem existir entre dois endereços de rede. Provisão de uma conexão de rede entre duas entidades de transporte. Multiplexação de múltiplas conexões de rede em uma única conexão de enlace de dados. Tratamento das atividades da camada de rede, inclusive ativação e controle de erros.

- **Transporte:** Colocação em sequencia das unidades de dados transferidas, para garantir que sejam entregues na mesma sequencia em que foram enviadas. Detecção de erros e recuperação após erros. Controle de fluxo de dados para evitar sobrecarga dos recursos da rede. Realização das atividades de supervisão da camada de transporte.

- **Sessão:** Provimento de um mapeamento um-para-um entre uma conexão de sessão e uma conexão de apresentação, em qualquer momento. Evitar que uma entidade de apresentação seja sobrecarregada de dados, pelo uso do controle de fluxo de transporte. Restabelecimento de uma conexão de transporte para suportar uma conexão de sessão. Realização das atividades de gerência da camada de sessão.

- **Apresentação:** Emissão de uma solicitação para que a camada de sessão estabeleça uma sessão. Iniciação da transferência de dados entre entidades de aplicação ou usuários. Execução de quaisquer transformações ou conversões de dados que forem requeridas. Emissão de uma solicitação para que a camada de sessão encerre a sessão.

- **Aplicação:** Execução das funções de aplicação comuns, que são funções que proporcionam capacidades úteis a muitas aplicações. Execução das funções de aplicação específicas, que são funções necessárias para atenderem aos requisitos de uma aplicação em particular.

O objetivo de uma estrutura de protocolo em níveis é delimitar e isolar funções de comunicações às camadas. Os dados transferidos em uma comunicação de um dado nível não são enviados diretamente (horizontalmente) ao mesmo nível da outra estação. O que sucede é o seguinte, os dados vão descendo camada por camada verticalmente pela máquina transmissora até atingir a camada ou nível físico (é neste nível físico que existe a única comunicação horizontal entre as máquinas). Quando os dados chegam à máquina receptora estes iniciam a subida vertical camada por camada até o nível de destino que, normalmente, será a camada de Aplicação desse computador.

A arquitetura da rede é formada por níveis, interfaces e protocolos.

Nível Físico

Fornece as características mecânicas, elétricas, funcionais e de procedimento para ativar, manter e desativar conexões físicas para a transmissão de bits entre entidades de nível de ligação possivelmente através de sistemas intermediários.

Uma unidade de dados do nível físico consiste de uma sequencia de bits, em uma transmissão serial, ou “n” bits conjuntos em uma transmissão paralela. Um exemplo de uma comunicação serial pode ser o acesso, via Telnet, para um terminal remoto, um exemplo de comunicação paralela é a comunicação entre uma impressora e uma CPU (computador).

Ao projetista de protocolos deste nível cabe decidir como representar os bits 0s e 1s, quantos microssegundos será a duração de um bit, se a transmissão será em modo Half-duplex ou Full-duplex, como a conexão será estabelecida e desfeita, quantos pinos terá o conector da rede e quais seus significados, bem como outros detalhes elétricos e mecânicos, tais como, o elemento condutor e os parâmetros que definem a transmissão. A função do nível físico é a de permitir o envio de uma cadeia de bits pela rede sem se preocupar com o significado desses bits ou como são agrupados.

Nível de Enlace de Dados (Data Link)

O objetivo deste nível é detectar e opcionalmente corrigir erros que por ventura ocorram no nível físico. O nível de ligação vai assim converter um canal de transmissão não confiável em um canal confiável para o uso do nível de rede. Quatro métodos são utilizados na delimitação dos quadros:

1. Contagem de caracter,
2. Transparência de caracter,
3. Transparência de bits e
4. Detecção de quadros pela presença ou ausência de sinal no meio físico.

Em geral todos os protocolos de nível de enlace incluem bits de redundância em seus quadros para detecção de erros, mas não a sua correção. Esta camada de enlace de dados executa a transferência de dados binários entre a camada física e a camada de rede. Em um computador pessoal, a placa de rede corresponde a essa camada.

Os dados que trafegam pela camada física são brutos, apenas sequencias de dígitos binários. Esta camada de enlace transforma esses bits em quadros (Frames) para serem processado pela camada de rede.

Nível de Rede

O objetivo deste nível é fornecer ao nível de transporte uma independência quanto a considerações de chaveamento e roteamento associados com o estabelecimento e operação de uma conexão de uma rede. Esta camada é responsável pelo endereçamento e tradução de nomes e endereços lógicos em endereços físicos. Ela determina a rota que os dados seguirão do computador de origem até o de destino. Tal rota dependerá das condições da rede, prioridade do serviço e outros fatores.

Também gerencia o tráfego e taxas de velocidade nos canais de comunicação. Outra função que pode ter é o agrupamento de pequenos pacotes em um único para transmissão pela rede (ou a subdivisão de pacotes grandes). No destino os dados são recompostos no seu formato original. Pode ser considerada uma das mais importantes, pois permitem que os dados cheguem ao destino da forma mais eficiente possível.

Nível De Transporte

Ao contrário da camada de rede, que entrega dados por toda a rede, a camada de transporte atua única e exclusivamente dentro do computador de cada usuário para entregar ou receber dados de um determinado processo ou aplicação específica.

O nível de rede não garante necessariamente que a cadeia de bits chegue ao seu destino. Pacotes podem ser perdidos ou mesmo reordenados. De forma a fornecer uma comunicação fim-a-fim verdadeiramente confiável é necessário outro nível de protocolo, que é justamente o nível de transporte. Este nível vai assim isolar os níveis superiores da parte de transmissão da rede.

As principais funções da camada de Transporte é o gerenciamento do estabelecimento e desativação de uma conexão, o controle de fluxo e a multiplexação das conexões.

Além das funções mencionadas, podemos ainda citar como funções deste nível o controle de sequencia fim-a-fim, a detecção e recuperação de erros fim-a-fim, a segmentação e blocagem de mensagens, entre outras. Portanto, o nível de transporte é o primeiro que trabalha com conexões lógicas fim a fim, ou seja, um programa na máquina de origem (fonte) conversa com um programa similar na máquina destino, diferente dos níveis anteriores, que conversavam somente com o nó vizinho. Vale ressaltar que a conexão criada pelo nível de transporte é uma conexão lógica.

As funções implementadas pela camada de transporte dependem da qualidade de serviço desejada. Foram especificadas, então, cinco classes de protocolos orientados à conexão:

1. **Classe 0**: Simples, sem nenhum mecanismo de detecção e recuperação de erros;
2. **Classe 1**: Recuperação de erros básicos sinalizados pela rede;
3. **Classe 2**: Permite que várias conexões de transporte sejam multiplexadas sobre uma única conexão de rede e implementa mecanismos de controle de fluxo;
4. **Classe 3**: Recuperação de erros sinalizados pela rede e multiplexação de várias conexões de transporte sobre uma conexão de rede;
5. **Classe 4**: Detecção e recuperação de erros e multiplexação de conexões de transporte sobre uma única conexão de rede.

Nível de Sessão

A função da camada de sessão é administrar e sincronizar diálogos entre dois processos de aplicação. Este nível oferece dois tipos principais de diálogo: Half-duplex e Full-duplex.

O nível de sessão fornece mecanismos que permitem estruturar os circuitos oferecidos para o nível de transporte. Neste nível ocorre a quebra de um pacote com o posicionamento de uma marca lógica ao longo do diálogo. Esta marca tem como finalidade identificar os blocos recebidos para que não ocorra uma recarga, quando ocorrer erros na transmissão.

Uma sessão permite o transporte de dados de uma maneira mais refinada que o nível de transporte em determinadas aplicações. Uma sessão pode ser aberta entre duas estações a fim de permitir a um usuário fazer o Login em um sistema remoto ou transferir um arquivo entre essas estações. Os protocolos desse nível tratam de sincronizações (Checkpoints) na transferência de arquivos.

Nível de Apresentação

A função da camada de apresentação é assegurar que a informação seja transmitida de tal forma que possa ser entendida e usada pelo receptor. Dessa forma, este nível pode modificar a sintaxe da mensagem, mas preservando sua semântica. Por exemplo, uma aplicação pode gerar uma mensagem em ASCII mesmo que a estação interlocutora utilize outra forma de codificação (como EBCDIC). A tradução entre os dois formatos é feita neste nível. A camada de apresentação também é responsável por outros aspectos da representação dos dados, como criptografia e compressão de dados.

Nível de Aplicação

A camada de aplicação é o nível que possui o maior número de protocolos existentes, devido ao fato de estar mais perto do usuário e os usuários possuírem necessidades diferentes.

Esta camada fornece ao usuário uma interface que permite acesso a diversos serviços de aplicação, convertendo as diferenças entre diferentes fabricantes para um denominador comum. Por exemplo, em uma transferência de arquivos entre máquinas de diferentes fabricantes pode haver convenções de nomes diferentes (por exemplo, antigamente o sistema operacional DOS tinha uma limitação de somente 8 caracteres para o nome de arquivo, o UNIX nunca teve essa limitação), formas diferentes de representar as linhas, e assim por diante.

Transferir um arquivo entre os dois sistemas requer uma forma de trabalhar com essas incompatibilidades, e essa é a função da camada de aplicação. O dado entregue pelo usuário à camada de aplicação do sistema recebe a denominação de SDU (Service Data Unit). A camada de aplicação, então, junta a SDU (no caso, os dados do usuário) um cabeçalho chamado PCI (Protocol Control Information). O objeto resultante desta junção é chamado de PDU (Protocol Data Unit), que corresponde à unidade de dados especificada de um determinado protocolo da camada em questão.

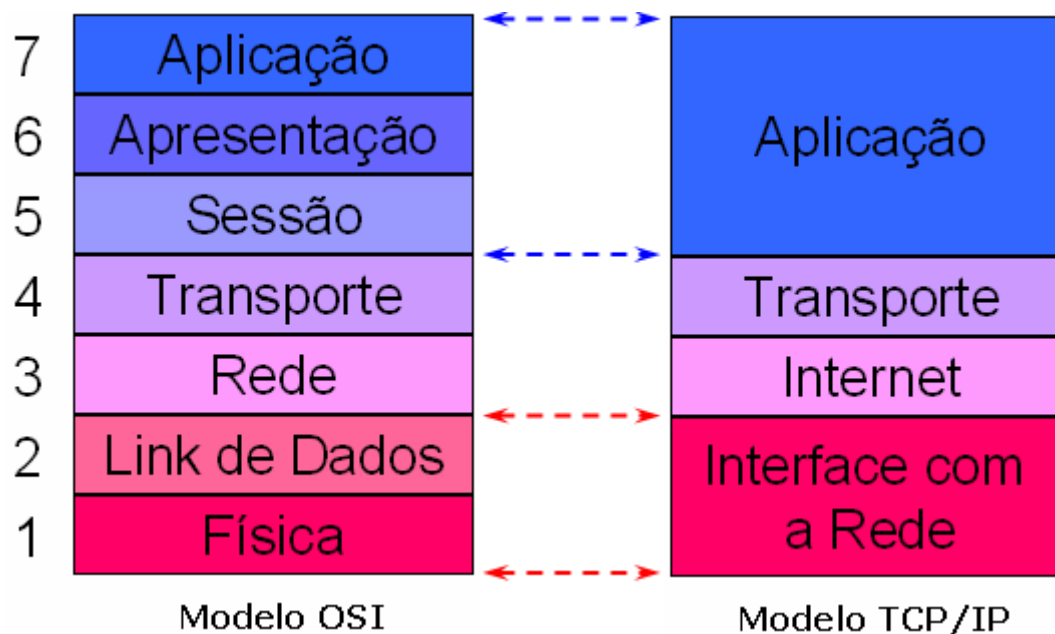
A tabela seguinte resume as funções das diferentes camadas do modelo OSI:

Camada	**Função**
(**7**) Aplicação	Funções especializadas (transferência de arquivos, Telnet, e-mail)
(**6**) Apresentação	Formatação de dados e conversão de caracteres e códigos.
(**5**) Sessão	Negociação e estabelecimento de conexão com outro nó.
(**4**) Transporte	Regras para a entrega de dados entre os extremos da conexão.
(**3**) Rede	Roteamento de pacotes através de uma ou várias redes.
(**2**) Enlace	Detecção e correção de erros introduzidos pelo meio de transmissão.
(**1**) Física	Transferência dos bits através do meio (canal) físico de transmissão.

A unidade básica de informação transmitida possui diversos "nomes" à medida que trafega entre as diferentes camadas, por exemplo:

- Bit (Binary Digit) (camada física, nível 1 do modelo OSI)
- Quadro ou Frame (camada de enlace, nível 2 do modelo OSI)
- Pacote, Datagrama (camada de rede, nível 3 do modelo OSI)
- Segmento (camada de Transporte, nível 4 do modelo OSI)

Modelo OSI vs. Modelo TCP/IP

O modelo TCP/IP quando comparado com o modelo OSI, tem duas camadas que se formam a partir da fusão de algumas camadas deste último, elas são: as camadas de Aplicação (Aplicação, Apresentação e Sessão) e Rede (Link de dados e Física). Veja na ilustração abaixo a comparação:

Conclusões sobre o Modelo OSI

Lembrar sempre que o modelo OSI não é um modelo físico, mas sim um modelo de referência aberto para desenvolvedores de Hardware/Software de rede. O objetivo do modelo OSI é fornecer uma base comum que permita o desenvolvimento coordenado de padrões para a interconexão de sistemas, onde o termo aberto não se aplica a nenhuma tecnologia, implementação ou interconexão particular de sistemas, mas sim à adoção dos padrões para a troca de informações, padrões esses que representam uma análise funcional de qualquer processo de comunicação.

A elaboração do modelo OSI representou um esforço na tentativa de padronização e direcionamento do desenvolvimento das novas tecnologias para a implementação de produtos de redes que fossem compatíveis entre si. Entretanto, o modelo OSI é um modelo de referencia, portanto, é um modelo conceitual e não uma arquitetura de desenvolvimento real de protocolos de rede. Por exemplo, a Internet se baseia em um modelo de quatro camadas onde não existe a estruturação formal dessas camadas conforme ocorre no modelo OSI. Ela procura definir um protocolo próprio para cada camada, assim como a interface de comunicação entre duas camadas adjacentes.

UNIDADE 14

Objetivo: Conhecer a extrema importância desta grande família de protocolos.

O Modelo TCP/IP (Parte I)

O desenvolvimento do sistema operacional UNIX possibilitou a criação da família de protocolos TCP/IP (Transmission Control Protocol/Internet Protocol) e dessa fusão nasceu a semente inicial da Internet, patrocinada pela Defense Advanced Research Projects Agency (DARPA) com o objetivo de se manter conectados mesmo que, apenas em parte, órgãos do governo e universidades. A ARPANET surgiu como uma rede que permaneceria intacta caso um dos servidores perdesse a conexão, e para isso, ela necessitava de protocolos (robustos) que assegurassem tais funcionalidades trazendo confiabilidade, flexibilidade e que fosse fácil de implementar e para tanto foi desenvolvida a arquitetura TCP/IP. Trata-se de um conjunto de protocolos desenvolvidos para permitir que computadores compartilhem recursos dentro de uma rede. Em uma definição mais básica, o nome correto para este conjunto de protocolos é “Conjunto de Protocolos para a Internet". Os protocolos TCP e IP são dois dos protocolos deste conjunto. Como os protocolos TCP e IP são os mais conhecidos, é comum se referir a TCP/IP para referenciar toda a família de protocolos.

Na família de protocolos TCP/IP, alguns protocolos, como TCP, IP e User Datagram Protocol (UDP), provêm funções de baixo nível, necessárias a diversas aplicações. Os outros protocolos executam tarefas específicas, como por exemplo, transferência de arquivos entre computadores, envio de mensagens. Os serviços TCP/IP mais importantes são:

- **Transferência de Arquivos**: O protocolo File Transfer Protocol (FTP), permite a um usuário em um computador copiar arquivos de um outro computador, ou enviar arquivos para um outro computador. A segurança é garantida requerendo-se que o usuário especifique um username e uma senha, para acesso ao outro computador.

- **Login Remoto**: O Network Terminal Protocol (TELNET), permite que um usuário se loga (tenha uma seção de trabalho) em um outro computador da rede. A seção remota é iniciada especificando-se o computador em que se deseja conectar. Até que a seção seja finalizada, tudo o que for digitado será enviado para o outro computador. O programa de TELNET faz com que o computador requisitante seja totalmente invisível, tudo é enviado diretamente ao computador remoto.

- **Worl Wide Web**: A rede mundial WWW estruturada. A estruturação de WWW e as normas (protocolos) e metodologias (HTML) de preparação de documentos para serem acessíveis e navegáveis pelas ferramentas de busca (Browser) disponíveis na Internet foram desenvolvidas originalmente para uso interno dos pesquisadores do CERN (Centro Europeu de Pesquisa Nuclear) e depois adotados como padrão internacional. Conjunto dos servidores que "falam" HTTP e informação aí armazenada em formato HTML. O World-Wide-Web é uma grande teia de informação multimídia em hipertexto. O hipertexto significa que se pode escolher uma palavra destacada numa determinada página e obter assim uma outra página de informação relativa. As páginas podem conter texto, imagens, sons, animações, etc. O WWW é uma gigantesca base de dados distribuída acessível de uma forma muito atraente e intuitiva.

O protocolo TCP/IP é baseado em um modelo que pressupõe a existência de um grande número de redes independentes com arquiteturas diferentes conectadas através de Gateways. Um usuário pode ter acesso a computadores ou outros recursos em qualquer uma destas redes. As mensagens, muitas vezes, passam por uma grande quantidade de redes para atingirem seus destinos. O roteamento destas mensagens deve ser completamente invisível para o usuário. Assim para ter acesso a um recurso em outro computador o usuário deve conhecer o endereço Internet deste computador. Atualmente este endereço é um número de 32 bits, escrito como 4 números decimais, cada um representando 8 bits de endereço.

Internet Protocol (IP)

O protocolo IP, padrão para redes Internet, é baseado em um serviço sem conexão. Sua função é transferir blocos de dados, denominados datagramas, da origem para o destino, onde a origem e o destino são hosts identificados por endereços IP. Este protocolo também fornece serviço de fragmentação e remontagem de datagramas longos, para que estes possam ser transportados em redes onde o tamanho máximo permitido para os pacotes é pequeno.

Como o serviço fornecido pelo protocolo IP é sem conexão, cada datagrama é tratado como uma unidade independente que não possui nenhuma relação com qualquer outro datagrama. A comunicação é não confiável, pois não são utilizados reconhecimentos fim-a-fim ou entre nós intermediários. Não são empregados mecanismos de controle de fluxo e de controle de erros. Apenas uma conferência simples do cabeçalho é realizada, para garantir que as informações nele contidas, usadas pelos Gateways para encaminhar datagramas, estão corretas.

Componentes TCP/IP

Um endereço IP é representado por um número binário de 32 bits, onde cada dígito binário pode ser apenas 0 ou 1. Os endereços IP são expressos como números decimais com pontos: divide-se os 32 bits do endereço em quatro octetos (um octeto é um grupo de 8 bits). O valor decimal de cada octeto varia desde 0 a 255 (11111111) sendo que estes extremos normalmente são utilizados para tarefas especiais.

A primeira parte do endereço identifica uma rede específica na inter-rede, a segunda parte identifica um host dentro desta rede. Este endereço, portanto, pode ser usado para nos referirmos tanto a redes quanto a um host individual. É através do endereço IP que os hosts conseguem enviar e receber mensagens pela rede, em uma arquitetura Internet TCP/IP.

Classes de Redes IP

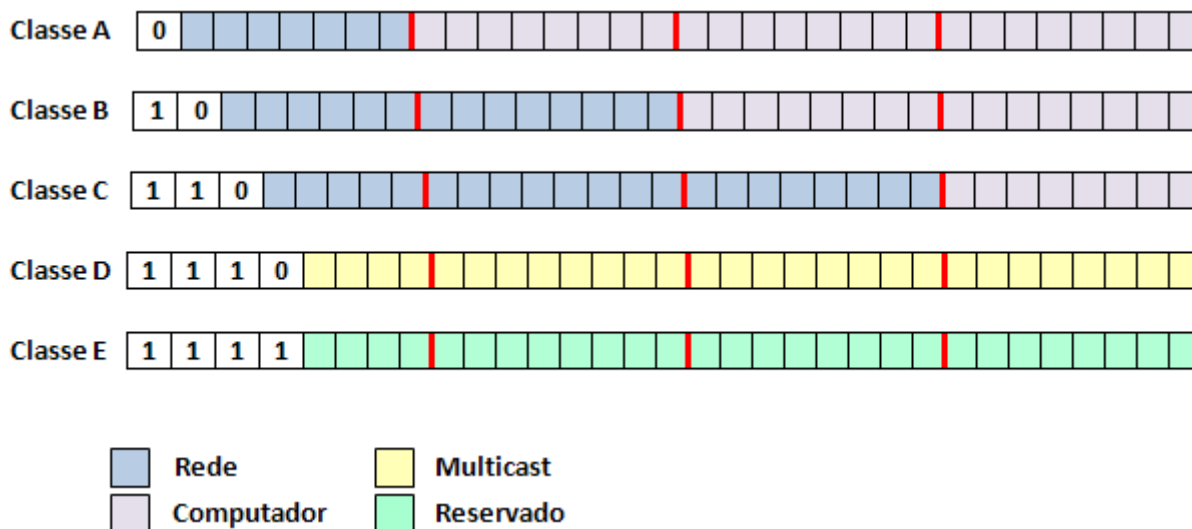
O protocolo IP utiliza três classes diferentes de endereços. A definição de classes de endereços deve-se ao fato do tamanho físico das redes LAN que são interligadas, ou seja, têm-se redes LAN com poucos computadores a redes públicas interligando milhares de máquinas. Na primeira classe de endereços, a classe A, o bit mais significativo é 0, os outros 7 bits do primeiro octeto identificam a rede, e os 24 bits restantes definem o endereço local. Essa classe é usada para redes de grande porte, seus endereços variam de 1 a 126, e cada rede tem capacidade de endereçar cerca de 16 milhões de hosts.

A classe B de endereços usa dois octetos para o número da rede e dois para endereços de hosts. Os endereços de redes classe B variam na faixa de 128.1 até 191.255 (os números 0 e 255 do segundo octeto, e 127 do primeiro octeto são usados para funções especiais e testes), e cada rede pode interligar (cerca de) 65 mil hosts.

Já os endereços classe C, utilizam três octetos para identificar a rede e apenas um octeto para o host. Os endereços de rede situam-se na faixa de 192.1.1 até 223.254.254 (os endereços acima de 223 no primeiro octeto foram reservados para uso futuro), e cada rede pode endereçar 254 hosts.

Classe	1º Byte	Número de Redes	Número de Máquinas/Sub-rede
A	**1 – 126**	**$2^7 - 2 = 126$**	**$2^{24} - 2 = 16.777.214$**
B	**128 – 191**	**$2^{14} - 2 = 16.382$**	**$2^{16} - 2 = 65.534$**
C	**192 – 223**	**$2^{21} - 2 = 2.097.150$**	**$2^8 - 2 = 254$**

As redes Classes D e E não são para uso comercial. A classe D serve para sistemas Multicast. Isto é, você só pode enviar dados para uma máquina que está configurada para tal propósito. A classe E serve para testes de novas implementações em redes TCP/IP.

A seguinte figura ajuda a visualizar essa diferença entre os diferentes tipos de Classes de redes, repare que a grande diferença entre uma Classe e outra reside no primeiro Byte do endereço IP.

Exemplo de um endereço IP binário Classe C de 32 bits (4 Bytes): **192.5.34.11**

11000000 • 00000101 • 00100010 • 00001011

$2^7\,2^6\,2^5\,2^4\,2^3\,2^2\,2^1\,2^0$ $2^7\,2^6\,2^5\,2^4\,2^3\,2^2\,2^1\,2^0$ $2^7\,2^6\,2^5\,2^4\,2^3\,2^2\,2^1\,2^0$ $2^7\,2^6\,2^5\,2^4\,2^3\,2^2\,2^1\,2^0$

Octeto (8 bits) Octeto (8 bits) Octeto (8 bits) Octeto (8 bits)

$(192 = 2^7+2^6) \bullet (5 = 2^2+2^0) \bullet (34 = 2^5+2^1) \bullet (11 = 2^3+2^1+2^0)$

Gateway Padrão

Para que um dispositivo se comunique com outro em outra rede, deve-se fornecer um Gateway padrão. Um Gateway padrão é o endereço IP da interface (placa de rede) do roteador, que se conecta ao segmento de rede onde se localiza o computador de origem. O endereço IP do Gateway padrão deve estar no mesmo segmento de rede da máquina de

origem. O Gateway padrão é um nó de rede que permite o acesso para outra rede, esta outra rede pode ser a Internet ou outra rede da mesma companhia. Neste caso um Gateway (padrão) é chamado de roteador porque os pacotes entrantes só sobem até a camada de rede (nível 3 do modelo OSI).

Máscara De Sub-Rede

A máscara de sub-rede informa aos dispositivos da rede que parte de um endereço é o campo da rede e que parte é o campo do computador. Normalmente uma máscara de sub-rede tem os bits iguais a 1 para a parte do endereço de rede e os bits iguais a 0 para a parte de endereçamento das máquinas, como esta máscara deve trabalhar com um endereço IP o tamanho dela será de 32 bits (4 Bytes).

A tabela abaixo mostra a máscara de sub-rede padrão para as redes Classe A, B e C. Os bits 1 (em vermelho) são utilizados para o endereço da rede e os bits 0 (em azul) servem para endereçar os computadores em cada sub-rede. É possível emprestar alguns bits 0 para criar sub-redes, quando isso acontece, a rede não esta mais fazendo uso da máscara padrão e sim de uma outra máscara de sub-rede que foi adotada devido às exigências e as particularidades de cada rede LAN. O número de bits emprestados indicara quantas sub-redes podemos criar dentro da nossa rede.

Classe	Máscara de Sub-rede Padrão	
A	**255.0.0.0**	**11111111.00000000.00000000.00000000**
B	**255.255.0.0**	**11111111.11111111.00000000.00000000**
C	**255.255.255.0**	**11111111.11111111.11111111.00000000**

CIDR (Classless Inter-Domain Routing)

O CIDR, foi introduzido em 1993, como um refinamento para a forma como o tráfego era conduzido pelas redes IP. Permitindo flexibilidade acrescida quando dividindo margens de endereços IP em redes separadas, promoveu assim um uso mais eficiente para os endereços IP cada vez mais escassos. O CIDR está definido no documento RFC 1519. O CIDR usa máscaras de comprimento variável, para alocar endereços IP em sub-redes de acordo com as necessidades individuais e não nas regras de uso generalizado em toda a rede. Assim a divisão de endereçamento de Rede (bits 1) e endereçamento de Computadores (bits 0) poderia ocorrer em qualquer fronteira de bits no endereço IP.

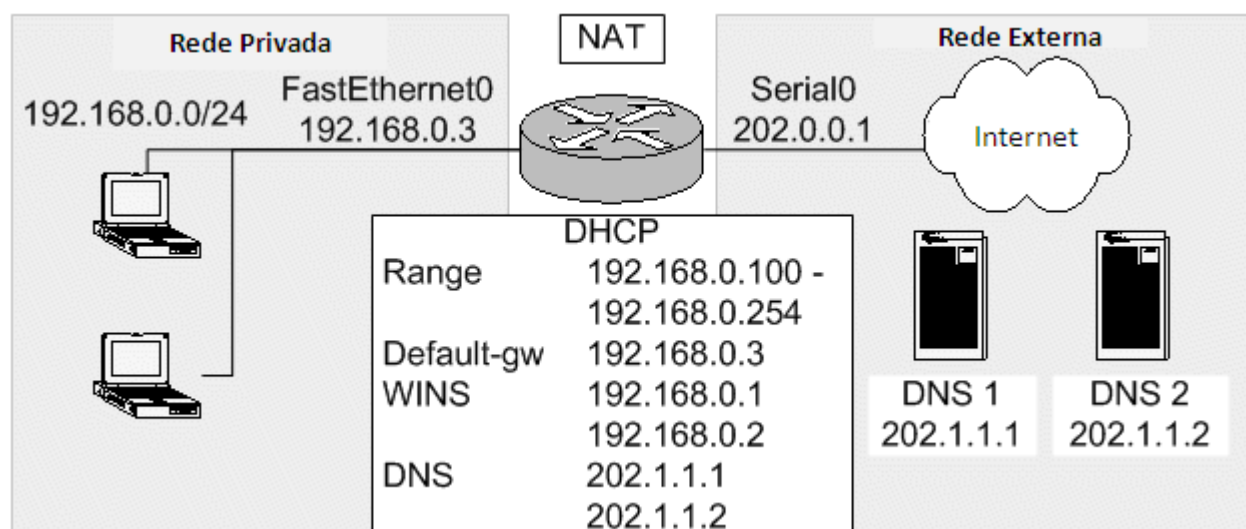
Devido a que as distinções de classes normais são ignoradas, o novo sistema foi chamado de roteamento sem classes. Isto levou a que o sistema original (aquele visto anteriormente) passasse a ser chamado de roteamento de classes. Um exemplo de um endereço IP na nomenclatura CIDR é: 192.168.0.0 /22, o número (/22) indica que estamos trabalhando com 22 bits (de valor 1) na máscara de sub-rede. Este IP representa os 1024 endereços IPv4 de 192.168.0.0 até 192.168.3.255 inclusive, com 192.168.3.255 sendo o endereço de Broadcast para essa rede.

Enquanto os endereços válidos da Internet estão se tornando escassos, empresas e indivíduos podem maximizar o uso do seu atual espaço de endereçamento e até mesmo expandir seu espaço através do uso de endereços privados. CIDR também pode ser usado para melhorar a segurança e aumentar o tempo de resposta da rede através do uso de sub-redes.

A referência para os endereços que podem ser utilizados sem coordenação prévia é o documento RFC 1918, "Address Allocation for Private Internets" (fevereiro de 1996). Estes três grupos de endereços IP privados são os seguintes:

1. Desde **10.0.0.0** até **10.255.255.255** (Classe A, prefixo 10.0.0.0**/8**)
2. Desde **172.16.0.0** até **172.31.255.255** (Classe B, prefixo 172.16.0.0**/12**)
3. Desde **192.168.0.0** até **192.168.255.255** (Classe C, prefixo 192.168.0.0**/16**)

Mantendo-se atualizado com as tendências em tópicos como CIDR e software de rede do Linux e Windows, a maioria dos obstáculos para conectividade Internet e Intranet podem ser facilmente contornados. Como o CIDR oferece a todos uma forma de maximizar o pouco que temos, endereços privados nos permitem a flexibilidade para expandir além dos endereços fornecidos pelos nossos Provedores de Serviços Internet.

O uso de qualquer um desses três grupos de endereços IP privados (não roteáveis) dentro de uma corporação esta intimamente ligado ao uso dos protocolos DHCP (Dynamic Host Configuration Protocol) e NAT (Network Address Translation).

UNIDADE 15

Objetivo: Entender como funciona o complexo protocolo TCP na Internet.

O Modelo TCP/IP (Parte II)

Transmission Control Protocol (TCP)

O TCP é um protocolo da camada de transporte da arquitetura Internet TCP/IP. O protocolo é orientado a conexão e fornece um serviço confiável de transferência de arquivos fim-a-fim. Ele é responsável por inserir as mensagens das aplicações dentro do datagrama de transporte, reenviar datagramas perdidos e ordenar a chegada de datagramas enviados por outro computador. O TCP foi projetado para funcionar com base em um serviço de rede sem conexão e sem confirmação, fornecido pelo protocolo IP.

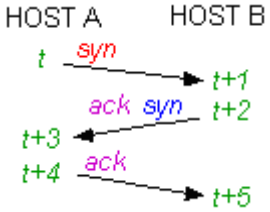
O protocolo TCP interage, de um lado, com processos das camadas superiores de aplicação e do outro lado com o protocolo da camada de rede do modelo da Internet. A interface entre o protocolo e a camada superior consiste em um conjunto de chamadas. Existem chamadas, por exemplo, para abrir e fechar conexões e para enviar e receber dados em conexões previamente estabelecidas. Já a interface entre o TCP e a camada inferior define um mecanismo através do qual as duas camadas trocam informações de maneira assíncrona.

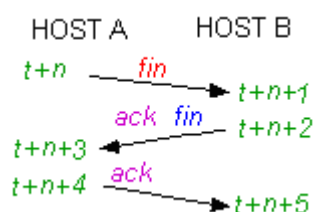
Este protocolo é capaz de transferir uma cadeia contínua de Bytes (Byte Stream), nas duas direções, entre seus usuários. Normalmente o próprio protocolo decide o momento de parar de agrupar os Bytes e de, consequentemente, transmitir o segmento formado por esse agrupamento.

Porém, caso seja necessário, o TCP pode requerer a transmissão imediata dos Bytes que estão no buffer de transmissão, através da função **push**. É bom enfatizar que para fazer uso desta função **push,** esta deve estar previamente habilitada no código fonte da aplicação (programa) em questão para que o TCP saiba como agir.

Conforme mencionado, o protocolo TCP não exige um serviço de rede confiável para operar, logo, responsabiliza-se pela recuperação de dados corrompidos, perdidos, duplicados ou entregues fora de ordem pelo protocolo de rede. Isto é feito associando-se cada Byte a um número de sequencia. O número de sequencia do primeiro Byte (dos dados contidos nesse segmento TCP) é transmitido junto com todo o segmento e é denominado número de sequencia desse segmento TCP. Como será explicado em breve, em toda conexão TCP tanto o transmissor como o receptor efetuam uma troca de segmentos. Isto é, Para cada segmento enviado existirá um segmento de reconhecimento emitido por parte do receptor. Portanto, os segmentos TCP emitidos pelo receptor para o transmissor trazem "de carona" (o que se conhece como Piggybacking) um reconhecimento positivo ACK (Acknowledgement) para informar que o segmento TCP enviado (pelo transmissor) foi recebido sem problemas.

O protocolo TCP realiza, além da multiplexagem, uma série de funções para tornar a comunicação entre origem e destino mais confiável.

São responsabilidades do protocolo TCP:

- O controle de fluxo,
- O controle de erro,
- A sequencia e a multiplexagem de mensagens.

A camada de transporte oferece para o nível de aplicação um conjunto de funções e procedimentos para acesso ao sistema de comunicação de modo a permitir a criação e a utilização de aplicações de forma independente da implementação. Desta forma, as interfaces Socket ou TLI (ambiente Unix) e Winsock (ambiente Windows) fornecem um conjunto de funções-padrão para permitir que as aplicações possam ser desenvolvidas independentemente do sistema operativo no qual funcionarão.

Estados De Uma Conexão TCP

Devido a que toda conexão TCP cria uma máquina de estados para o correto funcionamento da transferência de informação ponto a ponto é que vamos explicar em detalhe os diferentes estados de uma conexão TCP para viabilizar a análise do resultado da captura de pacotes na rede. Lembrar que cada estado do TCP é governando por temporizadores para que este não fique de forma indefinida em um determinado estado.

O TCP corresponde ao protocolo da camada de transporte do modelo de referência OSI que é orientado a conexão. Por ter essa característica, antes da transmissão de dados deve, necessariamente ser estabelecida uma sessão de comunicação entre o transmissor e o receptor.

Tempo	Evento	Diagrama
t	O computador A envia um pacote de sincronismo (**SYN**) para o computador B	
t+1	O computador B recebe o pacote (**SYN**) do computador A	
t+2	O computador B envia seu próprio pacote de sincronismo (**SYN**) e o reconhecimento (**ACK**)	
t+3	O computador A recebe o pacote **SYN** de B	
t+4	O computador A envia o seu pacote de reconhecimento positivo (**ACK**)	
t+5	O computador B recebe o **ACK**, e finalmente a conexão TCP é estabelecida e a transmissão dos pacotes de dados é iniciada até finalizar a sessão TCP.	

Essa sessão é estabelecida através de um processo chamado de 3-Way Handshake, esse processo sincronizará os números de sequencia além de oferecer informações de controle necessárias para o estabelecimento apropriado da conexão. A tabela anterior mostra o processo básico de processo 3-Way Handshake para o estabelecimento de uma conexão TCP. Se o processo de estabelecimento da conexão TCP não teve problemas, então a comunicação entre o cliente e o servidor está pronta e agora pode existir a troca de informação entre ambas as partes. A duração de uma conexão TCP é variável indo desde segundos, minutos até horas (ou mais). Em condições normais o encerramento de uma conexão TCP é iniciado pelo cliente enviando (ao servidor) um pacote FIN. A tabela abaixo ilustra este processo de finalização de uma conexão TCP após uma comunicação de **n** instantes de tempos entre o cliente e o servidor da Internet.

Tempo	Evento	Diagrama
t+n	O computador A envia um pacote de finalização (**FIN**) da conexão para o computador B	HOST A HOST B t+n fin t+n+1 ack fin t+n+2 t+n+3 t+n+4 ack t+n+5
t+n+1	O computador B recebe o pacote (**FIN**) do computador A	
t+n+2	O computador B envia seu próprio pacote de finalização (**FIN**) e (**ACK**) para o computador A	
t+n+3	O computador A recebe o pacote **FIN** e **ACK** de B	
t+n+4	O computador A envia o seu pacote de reconhecimento positivo (**ACK**) para o correto encerramento da conexão TCP	
t+n+5	Assim, o TCP ingressa ao estado de encerramento da conexão (Closed)	

UNIDADE 16

Objetivo: Entender quando é utilizado o protocolo UDP nas aplicações Internet.

O Modelo TCP/IP (Parte III)

User Datagram Protocol (UDP)

Muitas vezes não são necessários todos os recursos do protocolo TCP e alguns outros protocolos mais simples são utilizados em seu lugar. A alternativa mais comum é o protocolo UDP, designado para aplicações onde o usuário não necessita enviar sequencias longas de datagramas. Ele trabalha como o protocolo TCP, porém ele não divide os dados em múltiplos datagramas. Além disto, o protocolo UDP só mantém controle sobre os dados enviados quando o reenvio for necessário.

Na montagem do datagrama pelo protocolo UDP, o cabeçalho inserido é muito menor do que aquele inserido pelo protocolo TCP. O protocolo UDP opera no modo sem conexão e fornece um serviço de datagrama não confiável, sendo, portanto, uma simples extensão do protocolo IP. O UDP recebe os pedidos de transmissão de mensagens entregues pelos processos de aplicação da estação de origem, e os encaminha ao IP que é o responsável pela transmissão. Na estação de destino, o processo inverso ocorre. O protocolo IP entrega as mensagens (datagramas) recebidas ao UDP que as entrega aos processos de aplicação, sem nenhuma garantia.

O TCP/IP é um conjunto de protocolos para cuidar da informação transportada, sem distinção do tipo de hardware ou dados roteados entre várias redes ou a clareza da forma de aplicação, sendo desenvolvida pela Agência de Projetos e Pesquisas Avançadas de Defesa que iniciou assim o projeto da Internet. Os principais protocolos são TCP (Transmission Control Protocol) e IP (Internet Protocol), sendo hoje aceito e utilizado praticamente em todo o mundo.

A arquitetura TCP/IP implementa alguns "Serviços" que oferece aos usuários, mas é importante colocar em pauta que ela admite outros aplicativos que disponibilizem as mesmas facilidades.

O TCP/IP estabelece uma conexão fim-a-fim entre os usuários, isto significa o envio da mensagem com segurança entre o remetente e o destinatário. No transporte de arquivos o serviço de Correio Eletrônico só é útil para pequenas e rápidas quantidades de dados. O verdadeiro responsável pela transferência de arquivos volumosos entre sistemas na Internet, compatibilizando das desigualdades entre as aplicações das máquinas utilizadas, seria o FTP (File Tranfer Protocol), sendo um dos serviços da arquitetura TCP/IP. Embora seja um serviço de transferência de arquivos o FTP é, ao mesmo tempo, um protocolo do conjunto de protocolos TCP/IP.

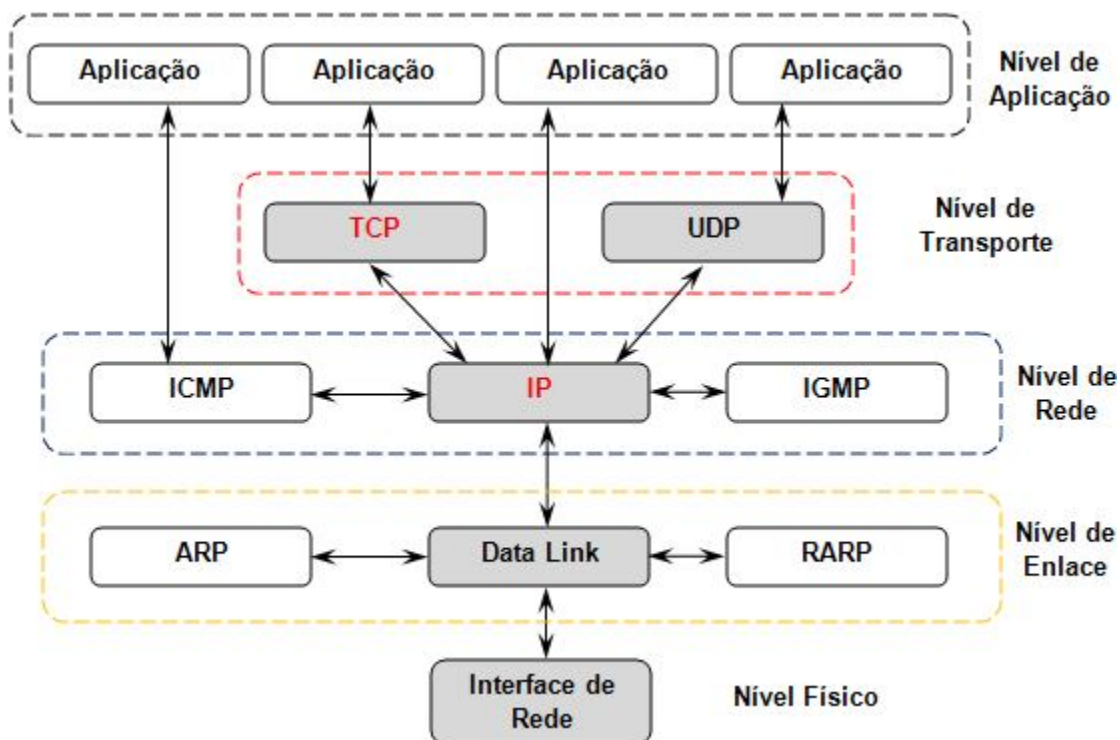
Uma aplicação (serviço) muito importante na arquitetura TCP/IP seria o "Telnet", este serviço aceita a conexão de uma máquina local em outra remota, gerando uma sessão interativa entre elas. Novamente aqui temos que o Telnet é tido como uma aplicação ou serviço da arquitetura TCP/IP, mas também o Telnet é um protocolo que faz parte dessa arquitetura.

O protocolo IP é responsável pelo serviço de interface com o hardware utilizado, por tal motivo facilita seu uso com várias plataformas (arquiteturas) de hardware. O protocolo IP gera uma unidade de transferência de dados, chamado Datagrama ou simplesmente pacote IP. Estes pacotes IP são "encapsulados" em diversos protocolos do nível de Enlace de Dados (Data Link), o nível de Data Link constitui-se, portanto, em uma interface relativamente simples entre a camada de rede (protocolo IP) e os protocolos do nível Físico, permitindo desta maneira que os pacotes IP sejam completamente independentes quanto à arquitetura física da rede na qual eles estão trafegando, por exemplo, a rede poderia ser uma Ethernet, FDDI, Token-Ring, etc.

Além dos mecanismos que possibilitam o controle de erros e confirmações positivas (ACK+) dos dados recebidos pelo destino, o protocolo TCP também facilita o controle de fluxo entre várias aplicações através do uso de portas bem conhecidas utilizadas pelas diferentes aplicações de rede. As facilidades do TCP/IP para com os usuários são várias, como por

exemplo, e só por citar algumas, o serviço de correio eletrônico (através dos protocolos SMTP, POP3), transferência de arquivos (FTP), Login para terminal remoto (Telnet, Secure Shell), transferência de Hipertexto (HTTP), etc.

Aplicações

As aplicações, no modelo TCP/IP, não possuem uma padronização comum. Cada uma possui um RFC próprio. O endereçamento das aplicações é feito através de portas (chamadas padronizadas a serviços dos protocolos TCP e UDP), por onde são transferidas as mensagens. Como mencionado anteriormente, é na camada de Aplicação que se trata a compatibilidade entre os diversos formatos representados pelos variados tipos de estações da rede.

A comunicação entre as máquinas da rede é possibilitada através de primitivas de acesso às camadas UDP e TCP. Antes de iniciar o estabelecimento da conexão, são executadas nessa

ordem, no servidor: As primitivas **socket** que cria um ponto terminal de comunicação e **bind** que registra o endereço da aplicação (número da porta). No cliente somente é executada a primitiva **socket**. Para estabelecer a conexão (com o protocolo TCP), a aplicação servidora executa a primitiva **listen**, ou seja, o servidor ficará sempre escutando as petições dos clientes. Do lado do cliente temos que cada vez que este efetue uma requisição ao servidor, deve executar a função **connect**. A aplicação servidora usa a primitiva **accept** para aceitar, receber e estabelecer a conexão do cliente. Já o UDP, como não é orientado à conexão, logo após o **socket** e o **bind**, utiliza as primitivas **send to** e **receive from**.

Principais Aplicações TCP/IP

Entre algumas das principais aplicações da família de protocolos TCP/IP podemos citar:

- **TELNET (Terminal Virtual)**: É um protocolo que permite a operação em um sistema remoto através de uma sessão de terminal. Com isso, a aplicação servidora recebe as teclas acionadas no terminal remoto como se fosse local. Utiliza a porta 23 do TCP. O TELNET oferece três serviços: Definição de um terminal virtual de rede, Negociação de opções (modo de operação, eco, etc.) e transferência de dados.
- **FTP (File Transfer Protocol)**: Provê serviços de transferência, renomeação e eliminação de arquivos, além da criação, modificação e exclusão de diretórios. Para sua operação, são mantidas duas conexões: uma de dados e outra de controle. Não implementa segurança, o que deixa para o TCP, exceto as requisições de senhas de acesso a determinados arquivos (ou servidores FTP). As transferências de arquivos podem ser no modo TEXTO (arquivos ASCII), onde há conversões de codificação para o sistema destinatário, e o modo BINÁRIO (arquivos executáveis), onde não há nenhuma conversão e todos os bytes são transferidos como estão.
- **SNMP (Simple Network Management Protocol)**: É utilizado para trafegar as informações de controle da rede. De acordo com o sistema de gerenciamento da arquitetura TCP/IP, existem o agente e o gerente que coletam e processam

respectivamente, dados sobre erros, problemas, violação de protocolos, dentre outros. Na rede existe uma base de dados denominada MIB (Management Information Base) onde são guardadas informações sobre máquinas, Gateways, interfaces individuais de rede, tradução de endereços, e softwares relativos ao IP, ICMP, TCP, UDP, etc. Através do SNMP é possível acessar aos valores dessas variáveis, receber informações sobre problemas na rede, armazenar valores, todos através da base do MIB.

- **DNS (Domain Name System)**: O DNS é um mecanismo para gerenciamento de domínios em forma de árvore. Tudo começa com a padronização da nomenclatura onde cada nó da árvore é separado no nome por pontos. No nível mais alto podemos ter: COM (organizações comerciais), EDU (instituições educacionais), GOV (instituições governamentais), MIL (órgãos militares), ORG (outras organizações), NET (Netwotking), etc. O DNS possui um algoritmo confiável e eficiente para tradução de mapeamento de nomes e endereços.

- **SMTP (Simple Mail Transfer Protocol)**: Implementa o sistema de correio eletrônico da Internet, operando via TCP é orientado à conexão, provê serviços de envio e recepção de mensagens do usuário. Tais mensagens são armazenadas num servidor de correio eletrônico onde o destinatário está cadastrado, até que este a solicite, quando são apagadas da área de transferência do sistema que originou a transferência. O SMTP divide a mensagem em duas partes: corpo e cabeçalho que são separados por uma linha em branco. No cabeçalho existe uma sequencia de linhas que identificam o emissor, o destinatário, o assunto, e algumas outras informações opcionais.

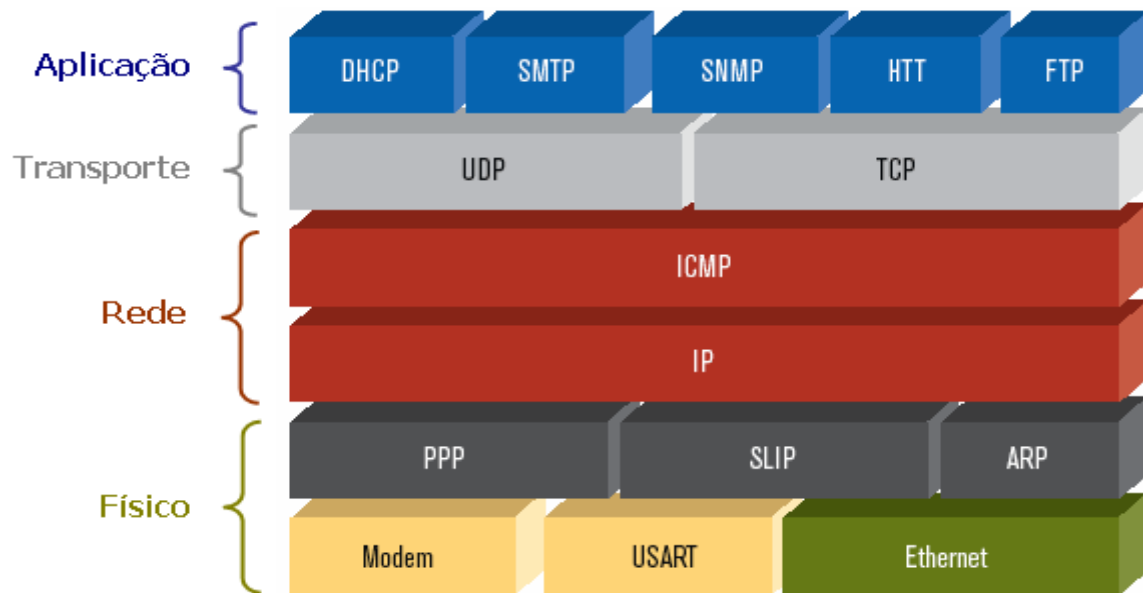
- **RPC (Remote Procedure Call)**: Implementa mecanismos de procedimentos de chamada remota, muito úteis no desenvolvimento de aplicações cliente-servidor com um nível de abstração maior. Uma aplicação utiliza o RPC para fazer interface das suas funções. Assim as funções chamadas pelas aplicações são repassadas ao RPC que monta uma mensagem correspondente e envia para processamento remoto. O servidor, então processa as mensagens, executa a rotina e devolve os resultados para

o RPC da estação, que reestrutura os dados e repassa à aplicação. Tudo isso implementa uma função virtualmente local, transparente para a aplicação.

- **NFS (Network File System)**: O NFS supre uma deficiência do FTP que não efetua acesso on-line aos arquivos da rede. Desenvolvido pela SUN Microsystems, tem acesso através da porta 2049 do UDP. O NSF cria uma extensão do sistema de arquivos local, transparente para o usuário e, desta forma, possibilita várias funções como as seguintes:
    - Criação e modificação de atributos dos arquivos;
    - Criação, leitura, gravação e eliminação de arquivos;
    - Criação, leitura e eliminação de diretórios;
    - Pesquisa de arquivos em diretórios;
    - Leitura dos atributos do sistema de arquivos.

  O sistema NFS é um recurso desenvolvido com o intuito de permitir a montagem de uma partição (ou disco rígido) que pertence a uma máquina remota, como se fosse uma partição local. Fornece, portanto, um método rápido e eficaz de compartilhar arquivos e espaço em disco entre máquinas distintas em uma rede. Devido a que o NFS faz uso do protocolo de transporte UDP, este tem embutidas várias rotinas de segurança para suprir a deficiência do UDP.

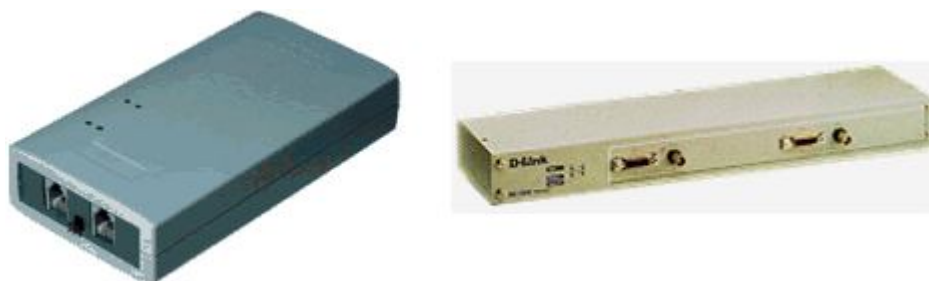
A grande flexibilidade e interoperabilidade fornecidas pela arquitetura TCP/IP, atraiu os fabricantes e fornecedores de recursos e o mercado de informática como um todo, pois, esta arquitetura, permite interconectar ambientes heterogêneos de forma eficiente e, com isso, todos passaram a usar esta tecnologia em larga escala.

A seguinte figura ilustra a maneira de exemplo visual, o modelo TCP/IP com alguns poucos dos seus protocolos do nível de Aplicação, relacionando a camada de Transporte e sua ligação física.

UNIDADE 17

Objetivo: Conhecer os equipamentos que fazem possíveis as conexões de rede.

Equipamentos De Rede (Parte I)

Repetidores

O termo repetidor remonta à época da comunicação visual, quando um homem situado em uma colina repetia o sinal que havia acabado de receber da pessoa na colina à sua esquerda, para comunicar o sinal à pessoa na colina à sua direita e assim sucessivamente até chegar ao destino desejado. Os repetidores foram (e ainda são) utilizados também nas comunicações telegráficas, telefônicas, por micro-ondas e ópticas, todas elas usam os repetidores para fortalecer seus sinais em longas distâncias, para que não acabem se enfraquecendo ou dissipando.

Basicamente, o objetivo principal de um repetidor é regenerar os sinais elétricos, tais como quadros Ethernet, que viajam pelo cabo de uma rede relativamente extensa, estes dispositivos primeiramente fazem a temporização (no nível de bit) do sinal entrante para poder amplificá-lo devidamente e assim habilitar esse sinal para que possa trafegar por uma distância maior através dos cabos da rede.

O primeiro meio popular de Ethernet foi um cabo coaxial de cobre conhecido como "Thick Ethernet" (Ethernet grosso ou espesso). O comprimento máximo desse cabo era de 500 metros (e 180 m para “thin Ethernet”). Em grandes prédios ou campus de universidades, um

cabo de 500 metros nem sempre era suficiente. Um **repetidor** resolve esse problema. Os repetidores conectam múltiplos segmentos de Ethernet, ouvindo cada segmento e repetindo o sinal ouvido para todos os outros segmentos conectados. O uso desses aparelhos permite aumentar significativamente o tamanho de uma rede. Os repetidores são dispositivos de porta única de "entrada" e porta única de "saída".

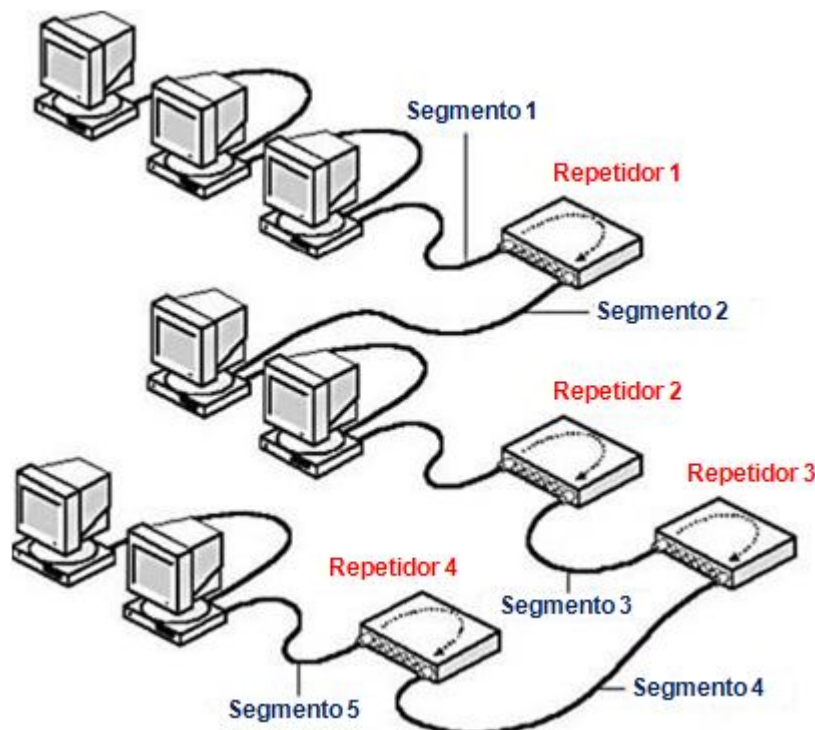
Existem muitos tipos de meios e cada um tem suas vantagens e desvantagens. Uma das desvantagens do tipo de cabo Cat5 UTP é o comprimento. O comprimento máximo do cabo UTP em uma rede é de 100 metros. Se precisarmos estender a rede além desse limite, devemos adicionar um dispositivo à rede. Esse dispositivo é o repetidor.

Em toda forma de transmissão de sinais elétricos, há a atenuação do sinal, que é a redução da amplitude do sinal devido, por exemplo, à resistência do cabo de cobre. Por isso, em um ambiente de Rede, existem limitações quanto ao comprimento do cabo. Por exemplo, numa Rede Local Ethernet, padrão 100Base-TX, a qual é amplamente utilizada, utilizando um Cabo Categoria 5, possui um limite de 100 metros de comprimento para cada segmento.

A função do repetidor, também conhecido como amplificador, é a regeneração de um sinal atenuado, e sua retransmissão. Este dispositivo, usado em redes locais, é usado para superar as limitações do meio físico utilizado, recebendo sinais atenuados por uma interface, regenerando-o e retransmitindo por outra interface.

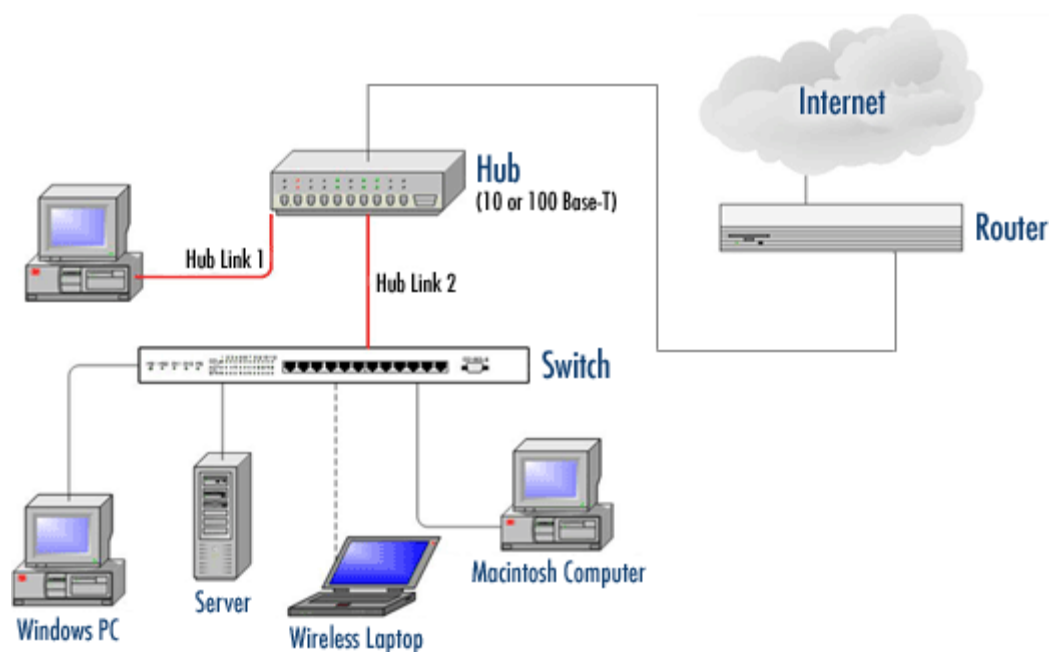
Os repetidores atuam na camada física (nível 1) do modelo OSI, isto se deve à característica de apenas atuarem diretamente com o sinal elétrico (bits), ou seja, com o meio físico propriamente dito. Um repetidor, não processa pacotes ou quadros, ele apenas atua como um regenerador de sinais, tratando assim de recuperar a potencia dos sinais elétricos.

Existem limites para o uso destes dispositivos em uma rede, pois como os repetidores não fazem nenhum tipo de filtragem dos pacotes transmitidos, eles apenas repassam tudo o que chega, os níveis de desempenho irão cair drasticamente à medida que novos nós sejam incluídos na rede, ou seja, o domínio de colisão irá se expandir.

Devido a esse problema, o padrão IEEE 802.3 implementa uma regra, conhecida como a regra 5-4-3, para o número de repetidores e segmentos em Backbones de acesso compartilhado Ethernet em uma topologia em árvore. A regra 5-4-3 gera dois tipos de segmentos físicos: segmentos povoados (pelos usuários da rede), e segmentos não-povoados (usados pelos links dos segmentos). Segmentos de usuários têm usuários de sistemas conectados a eles. Segmentos de link são usados para conectar os repetidores da rede juntos.

Basicamente, a regra 5-4-3 diz que toda rede pode conter 5 segmentos unidos por 4 repetidores, mas somente 3 desses segmentos podem ser povoados por estações. Os outros 2 segmentos restantes são usados como links entre repetidores. Repetidores podem ser usados para interligar segmentos Ethernet e estender a rede para um comprimento total de 925 metros. Como os repetidores não podem filtrar o tráfego da rede, ou seja, um bit visto em uma porta do repetidor é enviado para todas as outras portas. À medida que mais e mais clientes são acrescentados à rede, os níveis (volume) de tráfego aumentam. Como resultado, uma rede com muitos repetidores poderia ter um desempenho muito abaixo do nível ótimo.

Para fins de projeto, hoje em dia, raramente os repetidores são usados, isto devido ao barateamento dos Switches e também aos baixos níveis de desempenho em redes maiores. Porém, em redes pequenas, com baixo nível de tráfego, seu uso é aceitável.

Hubs E Switches

Os Hubs são dispositivos utilizados para conectar os equipamentos que compõem uma LAN. Com o Hub, as conexões da rede são concentradas (por isto também é chamado de concentrador) ficando cada equipamento num segmento próprio. O gerenciamento da rede é favorecido e a solução de problemas facilitada, uma vez que o defeito fica isolado no segmento de rede.

A finalidade de um Hub é gerar e retemporizar os sinais da rede novamente. Isso é feito no nível de bit para um grande número de computadores (por exemplo, 4, 8 ou mesmo 24) usando um processo conhecido como concentração. Você vai observar que essa definição é muito similar com a definição dos repetidores, por essa razão um Hub é também conhecido como repetidor multiportas.

A diferença é o número de cabos que se conectam ao dispositivo. Os motivos para se usar os Hubs é criar um ponto de conexão central para os meios de cabeamento e aumentar a confiabilidade da rede. Aumenta-se a confiabilidade da rede permitindo qualquer cabo único a falhar sem afetar toda a rede.

Os Hubs são considerados dispositivos da camada 1 porque apenas geram novamente o sinal e o transmite para suas portas (conexões da rede).

Existem diferentes classificações dos Hubs na rede. A primeira classificação é dizer se os Hubs são ativos ou passivos. A maioria dos Hubs modernos é ativo. Eles obtêm energia de uma fonte de alimentação para gerar novamente os sinais da rede. Alguns Hubs são denominados dispositivos passivos porque simplesmente repartem o sinal entre vários usuários, como usando um fio "Y" em um CD Player para usar mais de fone de ouvido. Os Hubs passivos não geram novamente os bits, ou seja, não estendem o comprimento de um cabo, apenas permitem um ou mais hosts se conectarem ao mesmo segmento de cabo.

Outra classificação é se os Hubs são inteligentes ou não. Os Hubs inteligentes têm portas de comunicação serial no console, o que significa que podem ser programados para gerenciar o tráfego da rede. Os Hubs não inteligentes simplesmente aceitam um sinal da rede de entrada e o repete em todas as portas sem a habilidade de realizar qualquer gerenciamento.

O Switch é um dispositivo de rede (Hardware) dotado de múltiplas portas para a conexão de comutação (Switching), ou seja, recebe dados de uma estação ou do próprio roteador conectado ao mundo externo (WAN) e os envia para as estações locais (LANs), conforme o endereço do destinatário. A taxa de transmissão é personalizada para cada usuário, até a capacidade total da banda do switch. O dispositivo é usado para conectar LANs entre si ou segmentar LANs, atuando normalmente na camada 2 (enlace de dados) do modelo OSI.

Quando se usa um Hub, as estações se comunicam pelo mesmo canal físico. Assim, existe a possibilidade de congestionamento e perda de tempo na retransmissão das informações. O Switch comutador corrige esse problema. Se, numa rede, um Hub dispõe de 10 Mbps para dividir entre todos os micros, um Switch com a mesma velocidade permite que cada equipamento se comunique com a velocidade (capacidade) total.

Hubs Inteligentes

Além dos Hubs comuns, que apenas distribuem os sinais da rede para os demais micros conectados a ele, existe uma categoria especial de Hubs, chamados de Smart Hubs, ou Hubs inteligentes.

Este tipo de Hub incorpora um processador e softwares de diagnóstico, sendo capaz de detectar e se preciso desconectar da rede estações com problemas, evitando que uma estação faladora prejudique o tráfego ou mesmo derrube a rede inteira; detectar pontos de congestionamento na rede, fazendo o possível para normalizar o tráfego; detectar e impedir tentativas de invasão ou acesso não autorizado à rede e outros problemas em potencial entre outras funções, que variam de acordo com a sofisticação do Hub. O SuperStak II da 3Com por exemplo, traz um software que baseado em informações recebidas do Hub, mostra um gráfico da rede, mostrando as estações que estão ou não funcionando, pontos de tráfego intenso, etc.

Usando um Hub inteligente a manutenção da rede torna-se bem mais simples, pois o Hub fará a maior parte do trabalho. Isto é especialmente necessário em redes médias e grandes.

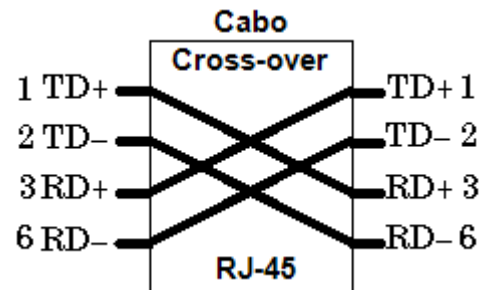
Conectando Hubs

A maioria dos Hubs possuem apenas 8 portas, alguns permitem a conexão de mais computadores, mas sempre existe um limite. E se este limite não for suficiente para conectar todos os micros de sua rede?

Para quebrar esta limitação, existe a possibilidade de conectar dois ou mais Hubs entre si. Quase todos os Hubs possuem uma porta chamada “Up Link” que se destina justamente a esta conexão. Para tal propósito é só conectar as portas de Up Link de ambos os Hubs, usando um cabo de rede normal para que os Hubs passem a se enxergar.

Como para toda a regra existe uma exceção, alguns Hubs mais baratos não possuem a porta Up Link, mas nem tudo está perdido, lembre-se do cabo Cross-over que serve para ligar

diretamente dois micros sem usar um Hub? Ele também serve para conectar dois Hubs. A única diferença neste caso é que ao invés de usar as portas Up Link, usaremos duas portas comuns.

Note que caso você esteja interligando Hubs passivos, a distância total entre dois micros da rede, incluindo o trecho entre os Hubs, não poderá ser maior que 100 metros, o que é bem pouco no caso de uma rede LAN de porte considerável. Neste caso, seria mais recomendável usar Hubs ativos, que amplificam o sinal.

Caso você precise unir dois Hubs que estejam muito distantes, você poderá usar um repetidor. Se você tem, por exemplo, dois Hubs distantes 150 metros um do outro, um repetidor estrategicamente colocado no meio do caminho servirá para viabilizar a comunicação entre eles.

Bridges (Pontes)

Uma Bridge é um dispositivo da camada 2 (do modelo OSI) projetada para conectar dois ou mais segmentos de uma rede LAN. A finalidade de uma Bridge é filtrar o tráfego em uma LAN, para manter local o tráfego local e, ainda assim, permitir a conectividade com outras partes (segmentos) da LAN para o tráfego para elas direcionado. Quando dois ou mais segmentos são conectados por uma Bridge o tráfego flui entre esses segmentos da LAN somente quando for necessário.

Portanto, é possível observar que uma característica muito útil das Bridges é a de segmentar uma rede LAN em vários segmentos (sub-redes), e com isto conseguem diminuir o fluxo de dados da rede. A aparência das Bridges varia muito dependendo do tipo. Embora tanto os roteadores assim como os Switches tenham assumido muitas das funções das Bridges, elas ainda continuam importantes em muitas redes. Para entender a comutação e o roteamento, é importante primeiro entender o funcionamento das Bridges.

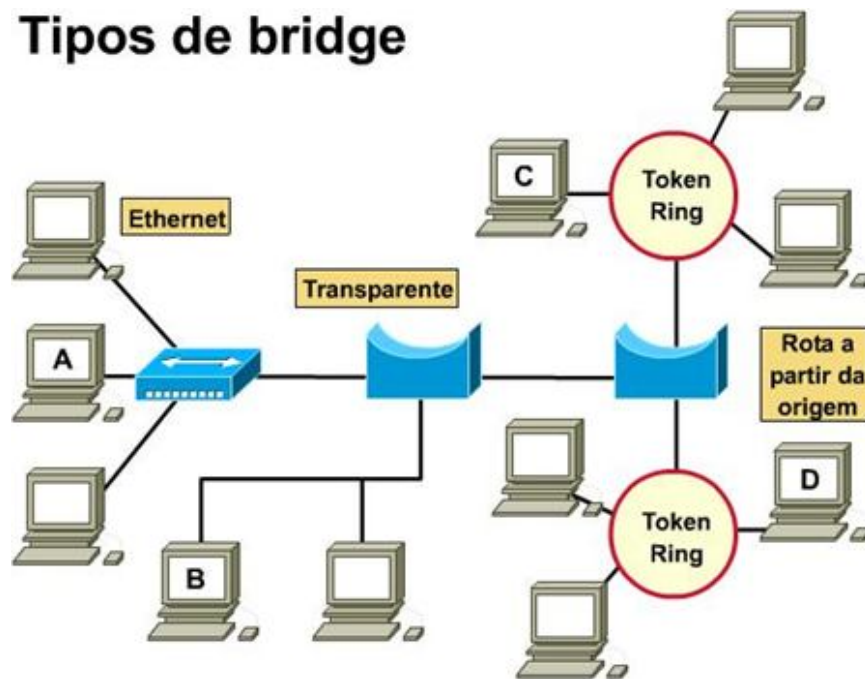
O que realmente define uma Bridge é a filtragem de quadros na camada 2, isto é, no nível de enlace de dados (Data Link). As Bridges também (em certas circunstancias) poderiam converter padrões, como por exemplo, de Ethernet para Token-Ring. Uma Bridge conecta os segmentos da rede e deve tomar decisões inteligentes sobre passar ou não sinais para o próximo segmento. Uma Bridge pode melhorar o desempenho da rede, eliminando tráfego desnecessário e minimizando as chances de colisões. A Bridge divide o tráfego em segmentos e o filtra com base na estação ou no endereço MAC.

As Bridges não são dispositivos complicados. Elas analisam quadros sendo recebidos, tomam decisões de encaminhamento com base nas informações contidas nos quadros e encaminham os quadros para o destino. As Bridges estão preocupadas apenas com a passagem ou não dos pacotes, com base em seus endereços MAC de destino. As Bridges frequentemente passam os quadros entre as redes, operando em diferentes protocolos da camada 2.

As Bridges manipulam pacotes, não retransmitindo ruídos, erros, e por isso não retransmitem quadros mal formados.

Funções Das Bridges

- Ler o endereço MAC dos quadros e retransmiti-los.
- Filtrar quadros, de modo que quadros com erros não sejam retransmitidos.
- Armazenam os quadros quando o tráfego for muito grande.

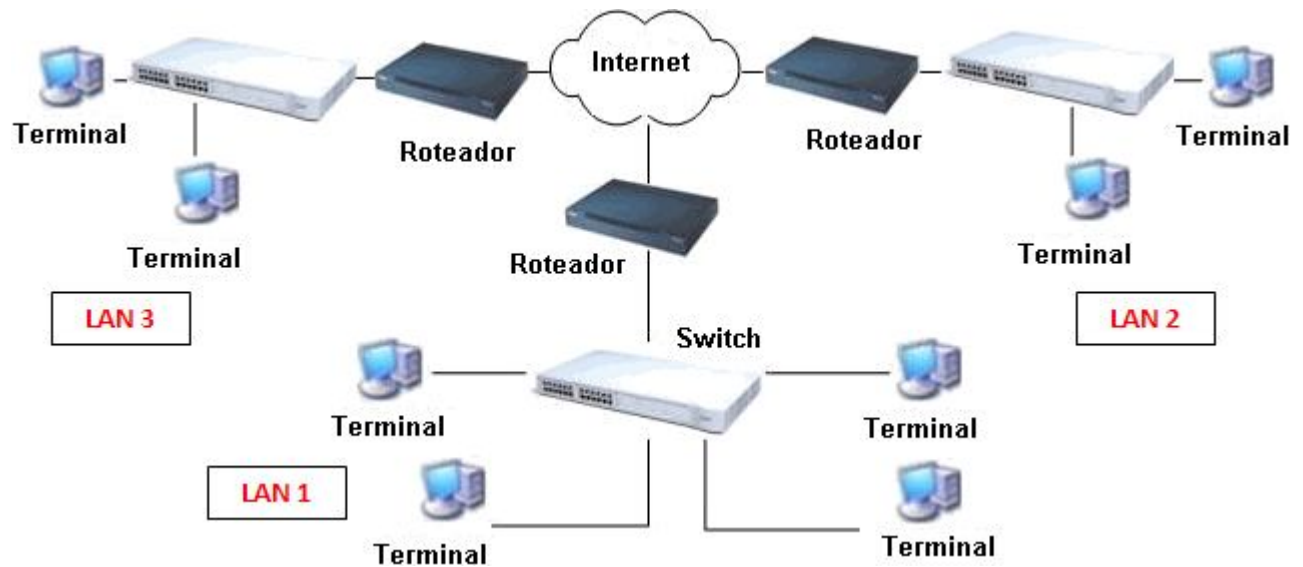
Em resumo, pode-se concluir que as Bridges são mais inteligentes que os Hubs. Analisa os quadros que chegam e os encaminha ou ignora baseado em informações de endereçamento físico (MAC Address). Coleta e repassa quadros entre segmentos de rede, mantém tabelas (temporárias) de endereços MAC.

Existem dois tipos diferentes de Bridges:

1. **As Bridges transparentes**: Este tipo de ponte pode ser utilizado sem alterar a configuração dos nós. Normalmente esses dispositivos não precisam nenhum tipo de configuração previa atuando como dispositivos do tipo Plug & Play. O funcionamento básico de uma ponte transparente é em modo promiscuo, isto é, capturando (e anotando) todos os quadros que se enviam por cada una das redes às que está conectado, independente de qual seja o endereço de destino.

2. **As Bridges rota a partir da origem**: Estes dispositivos foram muito utilizados principalmente pelas antigas redes LAN Token- Ring proprietária da IBM.

Roteadores

Estes dispositivos têm como finalidade escolher o melhor caminho para o tráfego de informações. Este caminho é decidido através de uma tabela interna que contém informações sobre a rede. Existem algoritmos que decidem sobre qual caminho deve ser tomado seguindo critérios que são conhecidos como "Métrica de Roteamento". Os

roteadores são também os nodos de uma rede, e são os responsáveis de concatenar diferentes tipos de redes LAN para formar uma WAN, portanto, são dispositivos muito importantes dentro da arquitetura e topologia de qualquer rede.

Entre as principais características temos:

- Grande memória interna;
- Armazenam grande quantidade de informação;
- Dispositivos para facilitar e controlar comunicação;
- Sistema de interrupção;
- Sistema de I/O assíncrono;
- Geralmente possuem um sofisticado Sistema Operacional;
- Software para controle de comunicação;
- Características de multiprogramação e esquemas de prioridade;

- Compartilhamento de recursos (processamento, programas, equipamento periférico, etc);
- Define os tipos de interconexões, sistema operacional, tipos de protocolos, e até os aplicativos a serem usados na rede.

Os roteadores trabalham na camada de rede (nível 3) do modelo OSI. Trabalhar na camada 3 permite ao roteador tomar decisões com base nos grupos de endereços de rede (endereços lógicos), ao contrário dos endereços (físicos) MAC individuais da camada 2.

Os roteadores também podem conectar diferentes tecnologias da camada 2, como Ethernet, Token-ring e FDDI. No entanto, devido à sua habilidade de rotear pacotes, com base nas informações da camada 3 (nível de rede), os roteadores se tornaram o Backbone da Internet, executando o protocolo IP (Internet Protocol).

A principal finalidade dos roteadores é examinar os endereços dos pacotes de entrada, escolher o melhor caminho para eles através da rede e depois comutar os pacotes para a porta de saída apropriada. Os roteadores são os dispositivos de controle de tráfego mais importantes nas grandes redes. Eles permitem que praticamente qualquer tipo de computador se comunique com qualquer outro computador em qualquer parte do mundo.

Funcionamento Dos Roteadores

Os roteadores iniciam e fazem a manutenção de tabelas de rotas executando processos e protocolos de atualização de rotas, especificando os endereços e domínios de roteamento, atribuindo e controlando métricas de roteamento. O administrador pode fazer a configuração estática das rotas para a propagação dos pacotes ou através de processos dinâmicos executando nas redes.

Os roteadores passam adiante os pacotes baseando-se nas informações contidas na tabela de roteamento. O problema da configuração das rotas estáticas é que, toda vez que houver

alteração na rede que possa vir a afetar essa rota, o administrador deve refazer a configuração manualmente. Já o conhecimento de rotas dinâmicas é diferente. Depois que o administrador fizer a configuração através de comandos para iniciar o roteamento dinâmico, o conhecimento das rotas será automaticamente atualizado sempre que novas informações forem recebidas através da rede. Essa atualização é feita através da troca de conhecimento entre os roteadores da rede.

Protocolos De Roteamento

São protocolos que servem para trocar informações de construção de uma tabela de roteamento. É importante ressaltar a diferença entre protocolo de roteamento e protocolo roteável. Protocolo roteável é aquele que fornece informação adequada em seu endereçamento de rede para que seus pacotes sejam roteados, como por exempo o IP (próprio da Internet) e o IPX (das redes Netware).

Um Protocolo de roteamento possui mecanismos para o compartilhamento de informações de rotas entre os diversos roteadores de uma rede, permitindo o roteamento dos pacotes de um protocolo roteável.

Entre os mais importantes protocolos de roteamento temos os seguintes:

- RIP v.1 e v.2 (Routing Information Protocol),
- OSPF (Open Shortest Path First),
- IGRP (Interior Gateway Routing Protocol),
- BGP (Border Gateway Protocol)
- EGP (Exterior Gateway Protocol), etc.

UNIDADE 18

Objetivo: Conhecer os diferentes equipamentos que fazem funcionar a uma rede.

Equipamentos de Rede (Parte II)

Placas de Rede

Uma placa de rede é um circuito impresso que se encaixa em um dos vários slots de expansão, com um determinado barramento (ISA, PCI, AGP, SCSI, etc), na placa mãe do computador ou em um dispositivo periférico.

Sua função é adaptar o computador ao meio da rede. Cada placa de rede em todo o mundo transporta um código exclusivo, conhecido como o endereço físico ou Media Access Control (MAC). Esse endereço é usado para controlar as comunicações de dados do host na rede.

Modems

A palavra Modem vem da conjunção das palavras **MOD**ulador **DEM**odulador, é um dispositivo eletrônico que transforma (modula) um sinal digital em uma onda analógica, pronta a ser transmitida pela linha telefônica, e que no lado do receptor o sinal analógico e

retransformado (demodulado) para o formato digital original. Utilizado para conexão com a Internet, sistemas BBS (Bulletin Board System), ou simplesmente para se conectar a outro computador.

Mesmo com o crescente aumento de conexões em banda larga, o modem do tipo "discado", que realiza uma chamada telefônica para se conectar ao provedor de Internet a 56 Kbps, ainda é muito usado.

O processo de conversão de sinais binários para analógicos é chamado de modulação digital para analógico. Quando o sinal é recebido pelo modem de recepção o processo é revertido (chamado demodulação). Ambos os modems devem estar trabalhando de acordo com os mesmos padrões, que especificam, entre outras coisas, a velocidade de transmissão em bps (bits por segundo), bauds, no nível do algoritmo de compressão de dados, tipo de protocolo de comunicação serial, etc. O prefixo Fax, na palavra Fax-Modem, se deve ao fato de que o dispositivo pode também ser utilizado para receber e enviar Fax.

Para transmitir os diversos tons pela linha telefônica é necessário convertê-los eletronicamente em um sinal analógico que varia gradualmente de frequência e potência. Os modems são utilizados para a transmissão de dados via uma linha telefônica de uma rede de comutação pública PSTN (Public Switched Telephone Network).

Basicamente, existem modems para acesso discado e banda larga. Os modems para acesso discado geralmente são instalados internamente em slots PCI da placa mãe do computador ou ligados externamente através de uma conexão serial, enquanto os modems para acesso em banda larga podem ser conectados através de portas USB ou placa de rede Ethernet utilizando cabo ou sem fio do tipo Wi-Fi (Wireless Fidelity).

Os modems ADSL (Asymmetric Digital Subscriber Line) diferem dos modems para acesso discado porque não precisam converter o sinal de digital para analógico e de analógico para digital devido a que o sinal transmitido já é digital.

Modem 56 Kbps PCI interno

Modem ADSL externo

Conexão e Funcionamento dos Modems (Conexão Discada)

Quando você configura seu modem para entrar em contato com o provedor de Internet, ocorre todo um processo de estabelecimento de comunicação entre seu computador e os servidores do provedor. Seu modem, após a discagem, emite uma série de barulhos para que a comunicação seja feita. Quando você usa algum software (como o Dial-Up no Windows e o kppp no Linux) para tentar se conectar à Internet, esse programa envia um sinal chamado DTR (Data Terminal Ready) para o modem instalado em seu computador. O modem "responde" enviando um sinal chamado DSR (Data Set Ready), que avisa o computador "que está tudo OK" para que uma conexão seja tentada.

O próximo passo é dado pelo software que gerencia a conexão, que envia ao modem uma instrução chamada TDL (Trasmit Data Line), que faz o modem abrir uma conexão com a linha telefônica. É um procedimento parecido com aquele quando retiramos o fone do gancho para fazer uma ligação. O software, após realizar esta ação, envia ao modem informações que indicam o número telefônico a ser discado e dados extras referentes à conexão com a Internet.

Quando o modem está estabelecendo uma conexão, um outro equipamento "responde": trata-se de um modem especial, ligado aos servidores do provedor de Internet. É neste instante que ocorre aquela série de ruídos, chamada de Handshaking (algo como "aperto de mãos"). Quando a conexão finalmente é estabelecida, o modem envia ao software gerenciador um sinal chamado de detecção de portadora CD (Carrier Detect), que permite ao computador enviar dados ao modem para que este os transmita.

Durante o Handshaking, uma série de "acordos" são estabelecidos: os dois modems (o do seu computador e o do provedor) determinam qual será a velocidade de transmissão de dados, qual a quantidade de bits por pacote, quantos bits serão usados para representar o início e fim de cada pacote, se um sistema de detecção de erros será usado, entre outros parâmetros necessários. Caso essas questões não sejam tratadas, a conexão pode ficar seriamente comprometida, já que um modem pode enviar dados mais rapidamente que o outro, a definição acerca dos pacotes de dados podem ter diferenças (e estas necessitam serem iguais), além de outros problemas, tais como, a finalização da conexão pelo modem do provedor.

Velocidade dos Modems

A baixa velocidade de transmissão de dados dos modems de conexão discada é uma das principais razões que levam uma pessoa ou uma empresa a utilizar uma conexão de banda larga. No entanto, os primeiros modems eram bem mais lentos que os atuais modems de 56 Kbps e naquela época, eram considerados verdadeiras revoluções da comunicação. Os primeiros modelos trabalhavam a 300 bauds (bauds é a unidade de medida que indica quantas vezes a frequência da transmissão varia durante um segundo, termo esse substituído por "Kbps").

A melhora na taxa de transferência teve alguns fatores importantes, dentre os quais o uso de linhas telefônicas equipadas com o sistema de tons ao invés do sistema de pulsos. Esse último tinha uma série de limitações e no caso da conexão com a Internet, era preciso

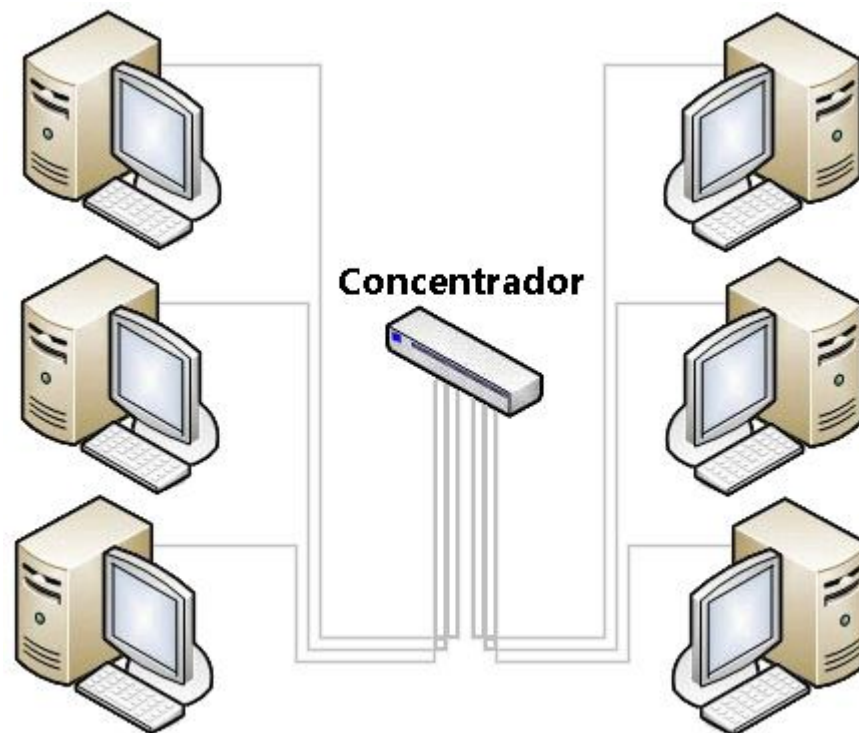
aguardar que um sinal chegasse até um modem para que o outro emitisse pacotes de dados. Esse problema já não ocorre mais.

Concentradores E Multiplexadores

O alto custo das linhas de comunicações é um dos maiores problemas na implementação de uma rede de comunicação de dados. Se cada terminal estiver ligado a um computador central através de um elo de comunicação independente, a atividade média em cada um desses elos será excessivamente baixa. O modo como os terminais são usados pode variar bastante e algumas linhas podem ficar inativas durante longos períodos de tempo, com nenhum ou pouquíssimo fluxo de informação entre o terminal e o computador. Se os períodos ativos das várias linhas nunca coincidem, é possível comutar uma única linha para atender a vários terminais.

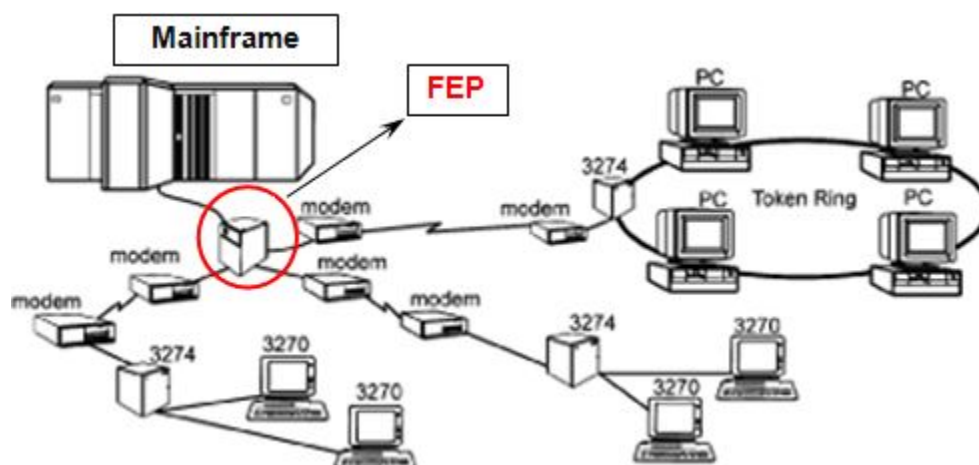
Esta é uma forma de multiplexação de mensagens. Porém, pode não ser sempre possível assegurar que somente um terminal esteja ativo em um dado instante de tempo, e se, nenhuma restrição é colocada no comportamento dos terminais conectados ao comutador, há necessidade de proporcionar uma linha saindo do comutador com uma capacidade maior do que a de qualquer linha de entrada. Se a capacidade da linha de saída excede a soma das capacidades de todas as linhas de entrada, o comutador executa a função de multiplexador.

A multiplexação pode ser efetivada dividindo-se a banda de frequência do canal de maior velocidade em várias bandas mais estreitas e alocando cada uma delas a um dos terminais. Essa forma de multiplexação (já estudada anteriormente) é conhecida como FDM (Frequency Division Multiplexing). Uma forma mais sofisticada consiste em amostrar cada linha oriunda de um terminal, sequencialmente, enviando o sinal recebido por um canal de alta velocidade. Essa forma é conhecida como TDM (Time Division Multiplexing), neste caso do TDM, a velocidade de transmissão oriunda de cada terminal não pode exceder a capacidade do canal que lhe foi alocado.

Outra modalidade de comutador de linha envolve o armazenamento das mensagens recebidas dos terminais para posterior envio ao computador central. Ele passa, então, a ser denominado concentrador, que é um dispositivo com buffer de armazenamento que altera a velocidade de transmissão de uma mensagem. Os concentradores geralmente são dotados de capacidade de processamento local, e sua velocidade é suficientemente rápida para que possam aceitar mensagens simultaneamente de vários terminais de baixa velocidade ou que possuam um fator de demanda baixo.

O concentrador atua como um coletor de mensagens dos usuários em uma área fisicamente próxima. As mensagens são montadas no buffer do concentrador até que este receba do usuário um delimitador. Juntamente com a mensagem é enviada a identificação do terminal. Sendo programáveis os concentradores remotos oferecem alta flexibilidade, permitindo acomodar interfaces para terminais especiais, proporcionando maior taxa de concentração, possibilitando atender a mudanças nas velocidades de transmissão nos formatos, nos códigos, nos protocolos de transmissão e no número de equipamentos terminais conectados.

Portanto, os concentradores chegam a ser outra modalidade de comutadores de linha, são multiplexadores inteligentes, possuem processador e um buffer de armazenamento onde armazenam os dados oriundos dos terminais para envio posterior ao servidor (aonde é enviada a identificação do terminal), o que altera a velocidade de transmissão de dados. Possuem capacidade de processamento local, e aceitam mensagens simultaneamente de vários terminais de baixa velocidade. Os concentradores incluem um software de controle, com isso um grande número de linhas (de baixa velocidade) pode compartilhar um pequeno número de linhas de alta velocidade, como são dispositivos programáveis oferecem:

- Alta flexibilidade, pois permitem interfaces para terminais especiais;
- Proporcionam maior taxa de concentração, possibilitando atender mudanças na velocidade, nos formatos, nos códigos, nos protocolos de transmissão e no número de terminais conectados.

Por exemplo, um tipo de concentrador é o processador do tipo Front-End, conhecido simplesmente como FEP (Front-End Processor), que executa as tarefas de processamento de comunicação e requisição de serviços, gerenciando a interface entre o servidor, geralmente um Mainframe, e os terminais clientes. Com isso é possível conseguir aumentar a disponibilidade do servidor para um processamento exclusivamente de dados.

Gateways

Um Gateway é uma máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos entre redes de arquiteturas diferentes.

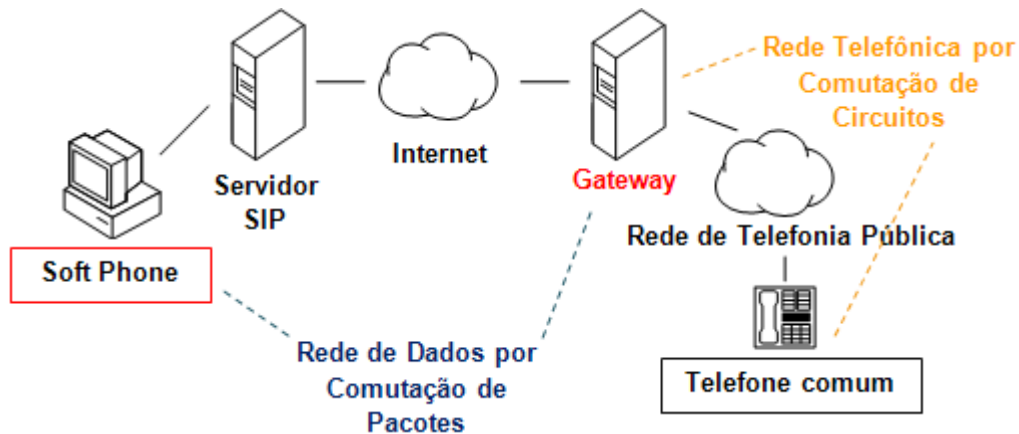
Exemplos de Gateway podem ser os routers (ou roteadores) e Firewalls, já que ambos servem de intermediários entre o usuário e a rede. Um Proxy também pode ser interpretado como um Gateway (embora em outro nível, aquele da camada em que opera), já que serve de intermediário também.

Portanto, um Gateway permite que os usuários da rede LAN tenham um acesso ao exterior por meio de linhas de transmissão de maior taxa de transferência, com o único objetivo de evitar possíveis congestionamentos entre a rede exterior e a rede local. Estas linhas de comunicações de alto desempenho se conectam nas portas WAN do Gateway. E, neste ponto de vista, estará dotado também de medidas de segurança contra invasões externas, como a utilização de protocolos codificados.

Cabe igualmente ao Gateway traduzir e adaptar os pacotes originários da rede local para que estes possam atingir o destinatário, mas também traduzir as respostas e devolvê-las ao par local da comunicação. Assim, é frequente a utilização de protocolos de tradução de endereços, como o NAT (Network Address Translation) que é uma das implementações de Gateway mais simples.

Regra Para Identificar O Tipo De Gateway

Uma regra simples diz que se os pacotes entrantes em um Gateway só atingem a camada de rede (nível 3 do modelo OSI) então esses Gateways são simples roteadores da Internet, portanto, é praticamente comum se ouvir falar de Gateways para se referir aos típicos roteadores que interconectam diferentes tipos de redes LAN, não é muito correto, mas o jargão de redes o permite. Porém, se os pacotes entrantes no Gateway vão além do nível 3 de rede chegando até as camadas superiores de aplicação, o que significa que os pacotes estão experimentando um processo de tradução de protocolos de uma rede com

determinada arquitetura (por exemplo, a Internet) para outro(s) protocolo(s) de rede com uma arquitetura muito diferente da primeira (por exemplo, a rede de telefonia celular ou fixa), portanto, quando ocorre isto, o dispositivo que realiza essa tradução é um Gateway verdadeiro.

Portanto, o conceito real de Gateway se dá aos equipamentos de comunicações eletrônicas que são utilizados para permitir a comunicação entre duas redes com arquiteturas diferentes. Evidentemente, a comunicação entre redes com arquiteturas diferentes pode gerar os mais diversos problemas, tais como:

- Tamanho máximo de pacotes;
- Forma de endereçamento;
- Técnicas de roteamento;
- Controle de acesso, etc.

UNIDADE 19

Objetivo: Saber quais são as ferramentas de gerenciamento de uma rede.

Gerenciamento de Redes

O contínuo crescimento em número e diversidade dos componentes das redes de computadores tem tornado a atividade de gerenciamento da rede cada vez mais complexa. Duas causas principais têm tornado árduo o trabalho de isolamento e teste de problemas:

1. Diversidade dos níveis do pessoal envolvido: técnicos, gerentes e engenheiros.

2. Diversidade nas formas de controle e monitoração: produtos cada vez mais complexos, cada fornecedor oferecendo ferramentas próprias de controle e monitoração.

As atividades básicas do gerenciamento de redes consistem na detecção e correção de falhas em um tempo mínimo e no estabelecimento de procedimentos para a previsão de problemas futuros. Por exemplo, é possível tomar medidas que evitem o colapso da rede, como a reconfiguração das rotas ou a troca do roteador por um modelo mais adequado, através da monitoração de linhas cujo tráfego esteja aumentando ou roteadores que estão se sobrecarregando.

A eficiência na realização destas tarefas está diretamente ligada à presença de ferramentas que as automatizem e de pessoal qualificado. Atualmente existem no mercado diversos tipos de ferramentas que auxiliam o administrador nas atividades de gerenciamento. Estas ferramentas podem ser divididas em quatro categorias:

1. Ferramentas de nível físico, que detectam problemas em termos de cabos e conexões de hardware.

2. Monitores de rede, que se conectam as redes monitorando o trafego.
3. Analisadores de rede, que auxiliam no rastreamento e correção de problemas encontrados nas redes.
4. Sistemas de gerenciamento de redes, os quais permitem a monetarização e controle de uma rede inteira a partir de um ponto central.

Dentre a gama de soluções possíveis para o gerenciamento de redes, uma das mais usuais consiste em utilizar um computador que interage com os diversos componentes da rede para deles extrair as informações necessárias ao seu gerenciamento.

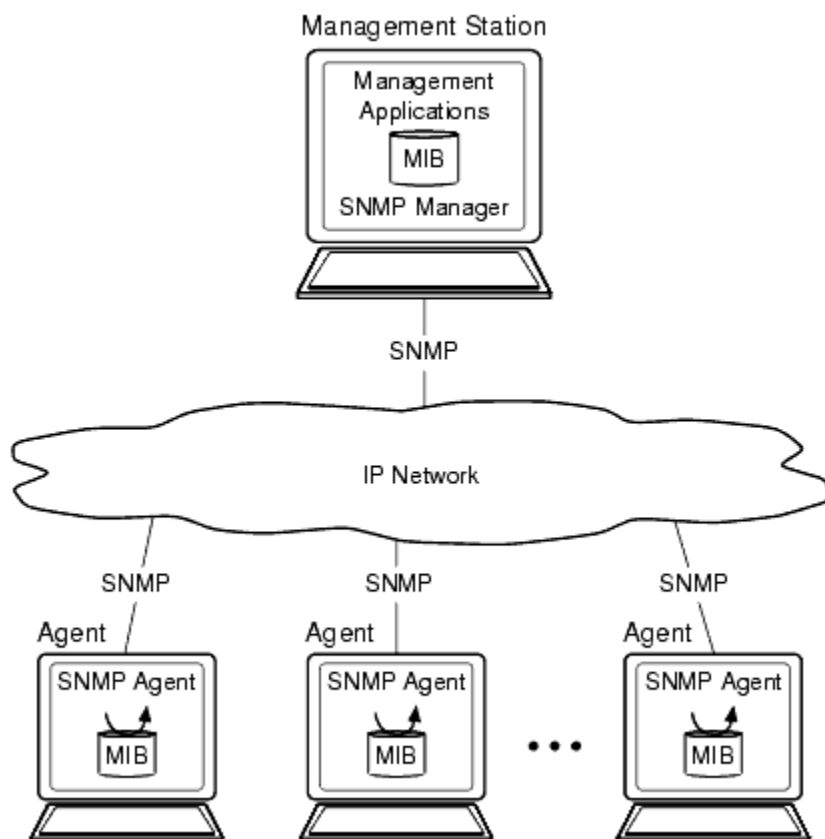
Evidentemente é preciso montar um banco de dados neste computador que será gerente da rede, contendo informações necessárias para apoiar o diagnóstico e a busca de soluções para problemas da rede. Isto envolve esforço para identificar, rastrear e resolver situações de falhas. Como o tempo de espera do usuário pelo restabelecimento do serviço deve ser o menor possível, tudo isto deve ser feito eficientemente.

Sistemas de Gerenciamento de Redes

Os sistemas de gerenciamento de redes apresentam a vantagem de ter um conjunto de ferramentas para análise e depuração da rede. Estes sistemas podem apresentar também uma série de mecanismos que facilitam a identificação, notificação e registro de problemas, como por exemplo:

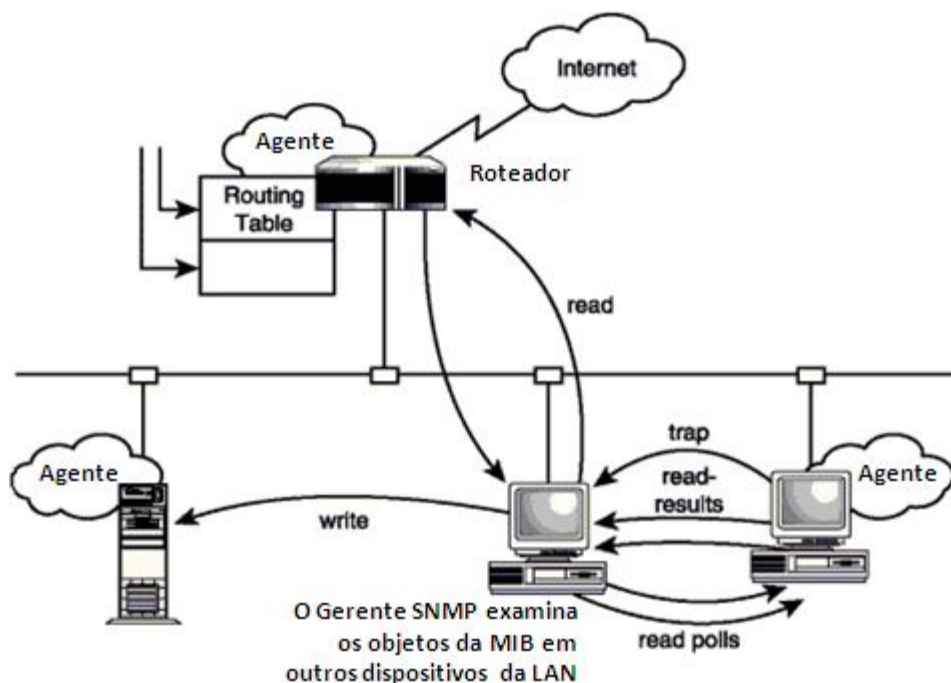
- Alarmes que indicam, através de mensagens ou bips de alerta, anormalidades na rede.
- Geração automática de relatórios contendo as informações coletadas.
- Facilidades para integrar novas funções ao próprio sistema de gerenciamento.

- Geração de gráficos estatísticos em tempo real.
- Apresentação gráfica da topologia das redes.

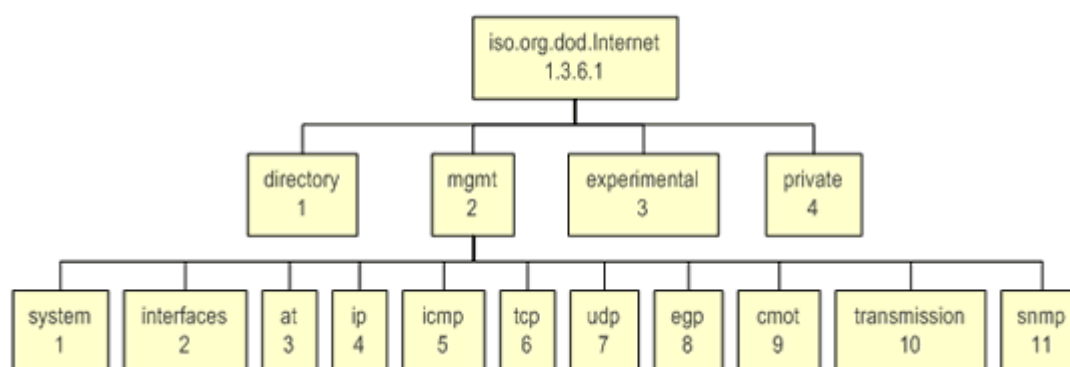
Em redes IP, o sistema de gerenciamento segue o modelo gerente-agente, onde o GERENTE é o próprio sistema de gerenciamento e o AGENTE é um software que deve ser instalado nos equipamentos gerenciados. A tarefa do agente é responder as requisições feitas pelo gerente em relação ao equipamento no qual o agente está instalado.

Esta interação é viabilizada pelo SNMP, o qual é como uma linguagem comum utilizada exclusivamente para a troca de informações de gerenciamento. Dessa forma, o gerente consegue conversar com qualquer máquina que fale SNMP, independente do tipo de

hardware e sistema operacional. O conjunto de informações ao qual o gerente pode fazer requisições ou alterações e denominado de MIB (Management Information Base).

O Protocolo SNMP - Simple Network Management Protocol

O protocolo de gerenciamento SNMP constitui atualmente um padrão operacional "de fato", e grande parte do seu sucesso se deve a sua simplicidade, sendo um protocolo send/receive com apenas quatro operações. Outro aspecto importante é a sua capacidade de gerenciar redes heterogêneas constituídas de diferentes tecnologias, protocolos e sistemas operacionais. Dessa forma, o SNMP pode gerenciar, por exemplo, redes Ethernet, Token-Ring e FDDI, conectando IBM PCs, Apple Machintosh, estações de trabalho SUN e outros tipos de computadores.

As aplicações de gerenciamento utilizam o SNMP para:

- Fazer polling nos dispositivos de rede e coletar dados estatísticos para análise em tempo real.
- Receber um conjunto limitado de notificações de eventos significativos ou mensagens do tipo trap. Uma mensagem trap é a única forma de um agente se comunicar com um gerente sem que este último tenha feito alguma solicitação.
- Reconfigurar dispositivos de rede.

Este protocolo tem como premissa à flexibilidade e a facilidade de implementação, também em relação aos produtos futuros. Sua especificação está contida no RFC 1157. O SNMP é um protocolo de gerência definido no nível de aplicação, é utilizado para obter informações de servidores SNMP - agentes espalhados em uma rede baseada na pilha de protocolos TCP/IP. Os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte UDP. Dentre as variáveis que podem ser requisitadas utilizaremos, normalmente, os objetos da MIB II que são os que nos permitirão gerenciar numa rede TCP/IP. Caso existam objetos de teste (ou privados) eles podem ser encontrados no diretório Experimental e Private, dentro deste último existe o diretório Enterprise que contem a MIB dos objetos proprietários das empresas que fabricam dispositivos de rede, tais como Cisco, 3Com, Nortel, etc. A estrutura de diretórios de gerenciamento da MIB é apresentada na seguinte figura.

O gerenciamento da rede através do SNMP permite o acompanhamento simples e fácil do estado, em tempo real, da rede, podendo ser utilizado para gerenciar diferentes tipos de sistemas. Este gerenciamento é conhecido como modelo de gerenciamento SNMP, ou simplesmente, gerenciamento SNMP. Por tanto, o SNMP é o nome do protocolo pelo qual as informações são trocadas entre a MIB e a aplicação de gerência como também é o nome deste modelo de gerência.

Os comandos são limitados e baseados no mecanismo de busca/alteração. No mecanismo de busca/alteração estão disponíveis as operações de alteração de um valor de um objeto, de obtenção dos valores de um objeto e suas variações. A utilização de um número limitado de operações, baseadas em um mecanismo de busca/alteração, torna o protocolo de fácil implementação, simples, estável e flexível. Como consequência reduz o tráfego de mensagens de gerenciamento através da rede e permite a introdução de novas características.

O funcionamento do SNMP é baseado em dois dispositivos o agente e o gerente. Cada máquina gerenciada é vista como um conjunto de variáveis que representam informações referentes ao seu estado atual, estas informações ficam disponíveis ao gerente através de consulta e podem ser alteradas por ele. Cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB.

Para operar, um agente SNMP deve estar presente em cada dispositivo da rede (roteador Switch, ou Hub, por exemplo), ou embutida na unidade ou como agente Proxy, sendo acessado por um terminal remoto. O SNMP não é um protocolo de Polling, ele espera para receber dados do dispositivo remoto ou envia dados por comandos de um operador. Basicamente ele troca informações por meio de mensagens (PDUs - Protocol Data Units), que possuem variáveis como nome e valor.

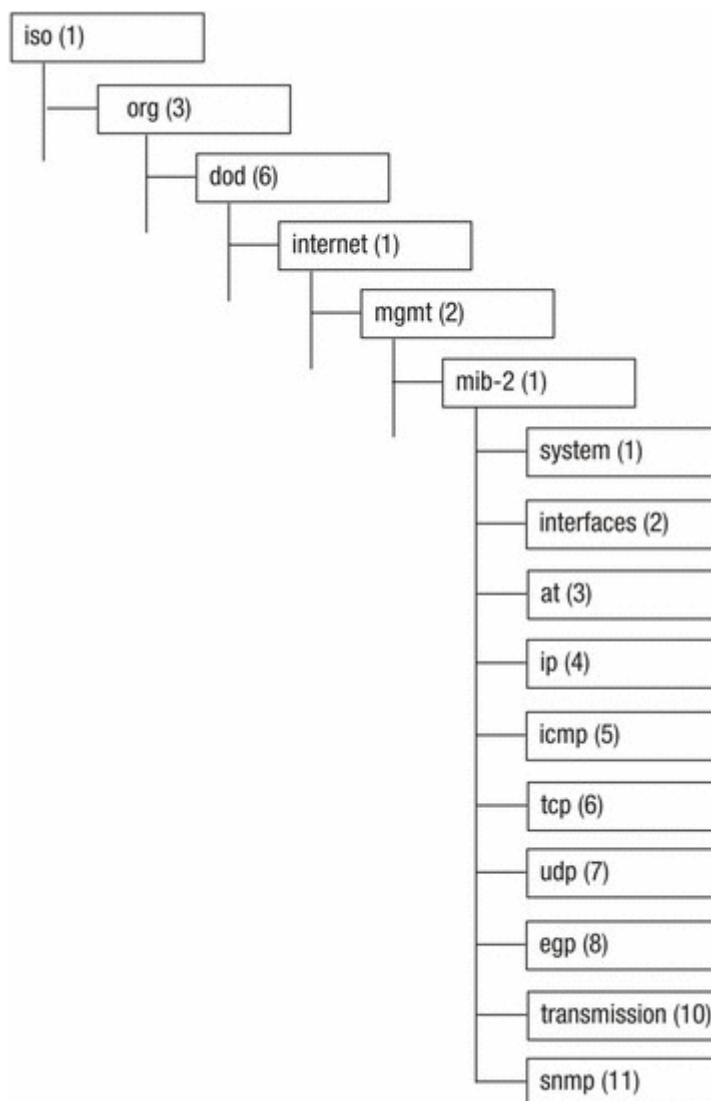
Esse protocolo opera com 4 tipos de PDUs,sendo:

- 2 tipos de GET (request) que coletam dados dos terminais;
- 1 SET que atribui valores aos dados dos terminais;

- 1 TRAP que monitora os eventos da rede (como o ligamento ou desligamento de um terminal da rede).

Como mencionado, o SNMP possui 3 elementos:

1. A MIB propriamente dita,
2. O manager (gerente SNMP) e
3. O agent (agent SNMP).

A MIB é um conjunto padrão de dados estatísticos e de controle, que descrevem o status do agente. Essa base de informação é estruturada como uma árvore, localizando-se no topo as informações mais gerais sobre a rede, ramificando-se nos detalhes e as folhas seriam os objetos propriamente ditos. Os objetos da árvore MIB podem assumir valores inteiros ou cadeias de caracteres (strings). A MIB está especificada na RFC 1156 e a MIBII na RFC 1213. Como exemplo, a figura apresenta parte do grupo de objetos da MIB II.

UNIDADE 20

Objetivo: Entender a arquitetura Cliente/Servidor, vantagens e desvantagens.

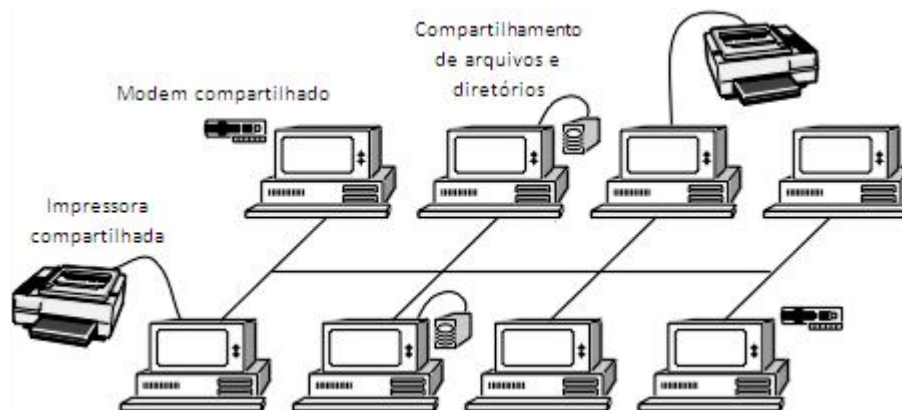
Servidores de Rede (Parte I)

Uma das funções básicas das redes locais é o compartilhamento de recursos caros e especializados (quer equipamentos, programas, base de dados, ou vias de comunicação), isto é: serviços, entre os vários usuários da rede.

Um servidor é um sistema de computação que fornece serviços a uma rede de computadores. Esses serviços podem ser de diversa natureza, por exemplo, arquivos e correio eletrônico. Os computadores que acessam os serviços de um servidor são chamados clientes. As redes que utilizam servidores são do tipo cliente-servidor, utilizadas em redes de médio e grande porte (com muitas máquinas) e em redes onde a questão da segurança desempenha um papel de grande importância. O termo servidor é largamente aplicado a computadores completos, embora um servidor possa equivaler a um software ou a partes de um sistema computacional, ou até mesmo a uma máquina que não seja necessariamente um computador.

A história dos servidores tem, obviamente, a ver com as redes de computadores. Redes permitiam a comunicação entre diversos computadores, e, com o crescimento destas, surgiu a ideia de dedicar alguns computadores para prestar algum serviço à rede, enquanto outros se utilizariam destes serviços. Os servidores ficariam responsáveis pela primeira função. Com o crescimento e desenvolvimento das redes, foi crescendo a necessidade das redes terem servidores e minicomputadores, o que acabou contribuindo para a diminuição do uso dos mainframes.

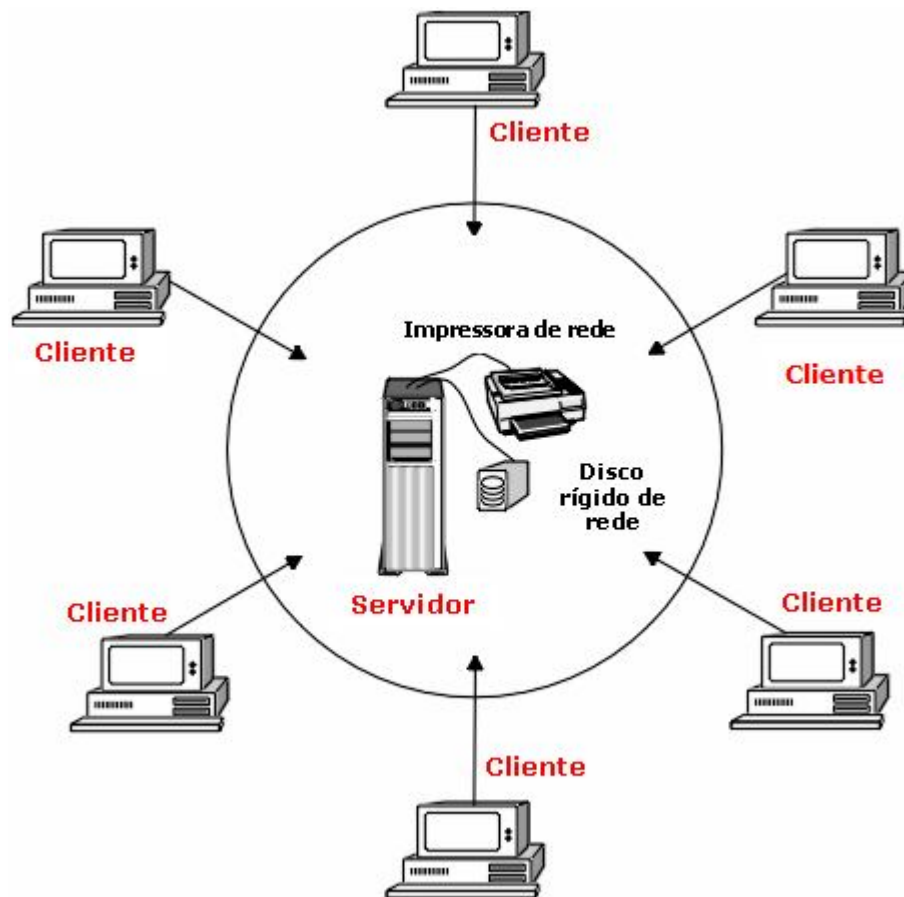
Qualquer estação de uma rede LAN pode oferecer serviço a outras estações (clientes). Vários serviços, dependendo do tipo de aplicação e estação de trabalho com um propósito específico, são projetados de forma a melhor oferecê-los. Tais servidores são distinguidos

das outras estações apenas pelo software que os suportam e algum hardware especial que contenham. Entre os serviços mais oferecidos podemos citar: o armazenamento de arquivos, a gerência de banco de dados, o suporte para impressão, a tradução de nomes simbólicos em endereços lógicos, concentrador de terminais, o suporte a telex, a monitoração de redes, a criptografia, o correio eletrônico, o suporte para teletexto, Gateways para outras redes e outras funções de hardware e software.

Servidores podem ser também clientes de outros servidores da rede. Por exemplo, o servidor de impressão pode ser cliente de um servidor de arquivo ao fornecer serviços aos seus próprios clientes. Serviço de correio eletrônico é outro exemplo de servidor que muitas vezes é realizado utilizando os serviços de armazenamento de arquivos de outro servidor.

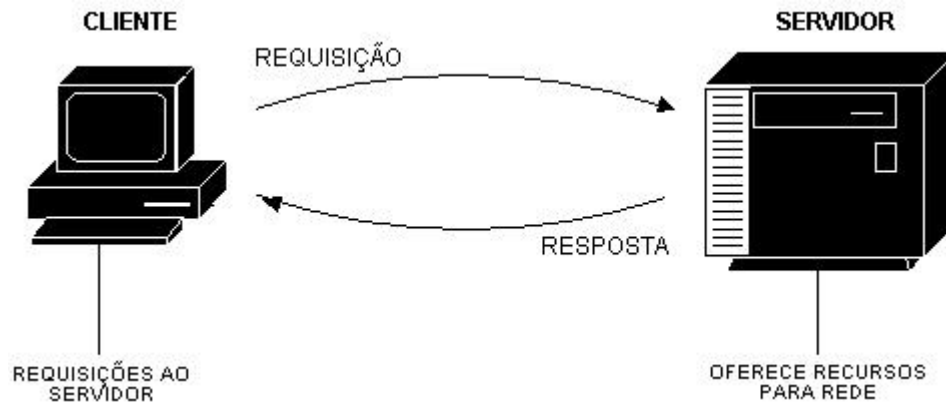
O crescimento das empresas de redes e o crescimento do uso da Internet entre profissionais e usuários comuns foi o grande impulso para o desenvolvimento e aperfeiçoamento de tecnologias para servidores.

Arquitetura Cliente/Servidor

Cliente/Servidor é um dos termos mais usados no mundo das redes informáticas no momento e pode ser sucintamente definido como um sistema de computação que utiliza três

componentes básicos para o compartilhamento de recursos: um computador-cliente, um computador-servidor e uma rede para conectá-los.

Tanto o cliente quanto o servidor podem ser computadores com variados graus de capacidade de processamento, que compartilham elementos de computação necessários para a execução do trabalho. Geralmente, o computador-cliente é um PC instalado na mesa de trabalho do usuário e o computador-servidor é um servidor de rede, podendo ser um PC avançado, um minicomputador (atualmente dito de médio porte), uma estação de trabalho ou um mainframe. A rede, local ou remota, pode ser qualquer uma capaz de estabelecer a comunicação entre os dois.

A comunicação entre cliente e servidor deve ser completamente independente da plataforma do servidor (hardware e software), bem como da tecnologia de comunicação utilizada (hardware e software). Por exemplo, um cliente DOS deve ser capaz de se comunicar da

mesma forma que um servidor UNIX ou OS/2, indiferentemente do sistema operacional do servidor e da tecnologia de LAN que conecta o cliente ao servidor.

Quando um sistema cliente/servidor utiliza mais de um servidor para atender e processar as requisições de informações emitidas pelos clientes tem-se um ambiente multiservidor.

Neste tipo de sistema, é conveniente e desejável que os servidores se comuniquem entre si para fornecerem serviços aos clientes sem que estes tomem conhecimento da existência de múltiplos servidores ou da comunicação intraservidor. Assim, tal como em um ambiente de processamento distribuído, o cliente não precisa se preocupar com o local onde sua consulta ou comando vai ser executado. Ele apenas solicita as informações e recebe os resultados.

Então, a arquitetura cliente/servidor divide uma aplicação em processos separados, executando em máquinas separadas, sobre uma rede. As tarefas definidas pelo usuário podem ser divididas em subtarefas a serem executadas ou pelo próprio cliente ou pelo(s) servidor(es), de acordo com os recursos proporcionados pelo sistema operacional de rede. Quanto mais avançado for este sistema operacional, menor será o tamanho da aplicação.

Por exemplo, o Microsoft LAN Manager possui um conjunto rico em funcionalidades voltadas para o desenvolvimento de sistemas cliente/servidor. Desta forma, uma aplicação cliente/servidor executando sobre o LAN Manager necessitará conter bem menos código, pois muitos dos recursos já são fornecidos pelo sistema operacional de rede. A consequência direta disso é a redução do tempo de desenvolvimento da aplicação.

Entretanto, se a mesma aplicação for executada sobre um sistema operacional de rede que proporcione um simples compartilhamento de arquivos e/ou de impressoras, o código dessa aplicação terá que implementar os recursos não propiciados pelo sistema, e neste caso, o código poderá até dobrar de tamanho, além de aumentar bastante o tempo gasto com o desenvolvimento do sistema.

Vantagens da Arquitetura Cliente/Servidor

Entre as principais vantagens da arquitetura Cliente/Servidor podemos mencionar:

- O software e o hardware dos PCs que estão cada vez mais baratos e mais poderosos, tornam-se um prato cheio para quem deseja implementar um Downsizing, pois o cliente/servidor permite que se utilize recursos de PCs, minicomputadores e mainframes, simultaneamente.
- Divisão mais eficiente do trabalho (parte do processo é realizada na porção Front-End e parte na Back-End), aqui os Front-End são os clientes e os Back-End são os servidores;
- Diminuição do tráfego de rede (apenas o resultado das consultas é transmitido do servidor ao cliente);
- O desenvolvimento de aplicações que utilizam GUI, nos mais diversos ambientes, incrementou sensivelmente a qualidade dos sistemas do ponto de vista do usuário final;
- Os usuários não ficam limitados a um tipo de sistema operacional ou plataforma e, com isso, podem continuar usando os softwares já conhecidos para acessar o banco de dados;
- Os dados podem ser protegidos contra perdas ou acessos indesejados, uma vez que o processamento dos mesmos é centralizado e executado por um sistema gerenciador

de banco de dados, projetado para esta tarefa, proporcionando assim, segurança e integridade, entre outros aspectos;

- Os clientes podem acessar mais dados, devido à versatilidade do SQL no acesso a dados em diferentes plataformas (padronização e portabilidade).

Desvantagens

- Aumento do custo administrativo e de pessoal de suporte para manter o servidor de banco de dados. Como este tipo de arquitetura possibilita a interação entre diferentes plataformas, em alguns casos, poderá haver um custo adicional com treinamento para familiarização do grupo de suporte com novas plataformas e/ou sistemas operacionais;

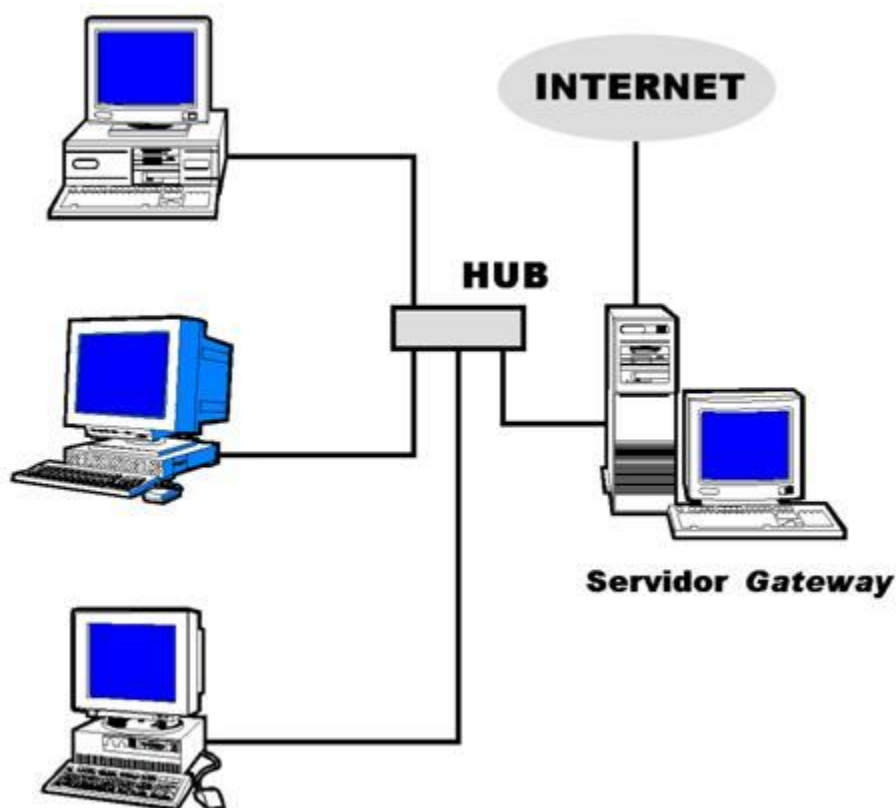
- Aumento do custo de hardware, principalmente quando se deseja manter um nível razoável de performance do sistema, o que torna necessário a disponibilidade de uma máquina dedicada executando o servidor de banco de dados, com recursos suficientes para proporcionar o desempenho esperado. Soma-se a isso a necessidade de equipamentos de suporte para proteção contra falta de energia;

- O custo do software do servidor do banco de dados, além dos aplicativos auxiliares e ferramentas de desenvolvimento, os quais serão mais caros se comparados aos servidores de arquivos;

- Devido à complexidade e ao grande número de partes que compõem um sistema cliente/servidor, torna-se mais difícil a identificação de pontos problemáticos e a configuração do sistema.

Aplicações

O emprego da tecnologia Cliente/Servidor depende de vários fatores: entre eles o objetivo ao qual se quer alcançar, o montante de investimento a ser feito, os recursos humanos (pessoas envolvidas), as aplicações a serem desenvolvidas e implantadas e o tempo de implantação do projeto.

As aplicações são: Internet, Intranet, Sistemas de Gerenciamento de Documentos, Sistemas de Apoio a Decisão, Sistemas Gerenciamento, Correio Eletrônico, Servidores de Fax, Servidores de Impressão, Gateways, Servidores de Arquivos, Servidores de Aplicações, Servidores de Banco de Dados, enfim, Servidores de Informação.

UNIDADE 21

Objetivo: Conhecer o funcionamento, o Hardware e Software dos Servidores.

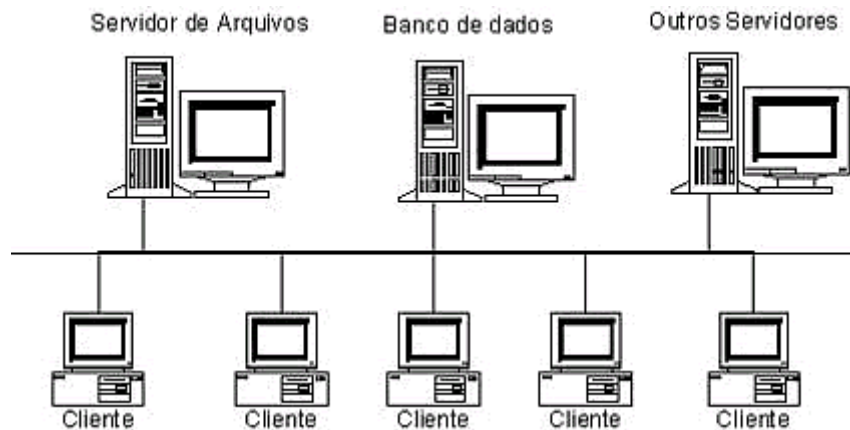
Servidores de Rede (Parte II)

Tipos de Servidores

Existem diversos tipos de servidores, entre os mais conhecidos e utilizados na Internet temos os seguintes:

- **Servidor de arquivos**: Servidor que tem como função oferecer aos seus clientes o serviço de armazenamento e acesso a informações e de compartilhamento de disco. Controlam unidades de disco ou outras unidades de armazenamento, sendo capazes de aceitar pedidos de transações das estações clientes e atendê-los utilizando os seus dispositivos de armazenamento. Um Servidor de Arquivo Geral é aquele que é capaz de aceitar transações, independente do sistema operacional do cliente, ou seja, independente da estrutura de arquivos da estação cliente. Neste caso, existe um sistema de arquivo padrão da rede, utilizado pelo servidor de arquivos, nos quais os vários arquivos das demais estações da rede devem ser convertidos (pelos protocolos no nível de apresentação) para comunicação com o Servidor. Sendo adotada esta solução, todos os arquivos da rede são potencialmente acessíveis a todas as estações, independente das estruturas de arquivos individuais.

- **Servidor de impressão**: Servidor responsável por controlar pedidos de impressão de arquivos dos diversos clientes. Um Servidor de Impressão típico tem vários tipos de impressoras acoplados, cada uma delas, adequada à qualidade ou rapidez de uma aplicação em particular. Existem várias formas de se implementar um Servidor de Impressão. A forma mais simples é baseada na pré-alocação da impressora. Neste caso uma estação cliente envia um pedido ao Servidor, manifestando o desejo de uso de uma impressora específica. Caso esta impressora esteja disponível, ela então é

alocada ao cliente até que este a libere (ou, então, até que se esgote o tempo máximo da utilização, conforme negociação na alocação). Caso a impressora não esteja disponível o cliente é avisado e colocado, se é de seu desejo em uma fila de espera. Uma outra forma de implementarmos um Servidor de Impressão é utilizando a técnica de Spooling. Neste caso a estação ao invés de pedir a alocação de uma impressora, envia diretamente ao Servidor o texto a ser impresso. Este texto é colocado em uma fila de espera, sendo impresso quando a impressora estiver disponível.

- **Servidor de rede**: Encarregado da monitoração do tráfego, do estado dela, do desempenho de uma estação da rede, assim como ver o estado do meio físico de transmissão e outros sinais, também faz o gerenciamento da rede de forma a possibilitar a detecção de erros, diagnose e resoluções de problemas da rede, tais como falhas, desempenho, etc.

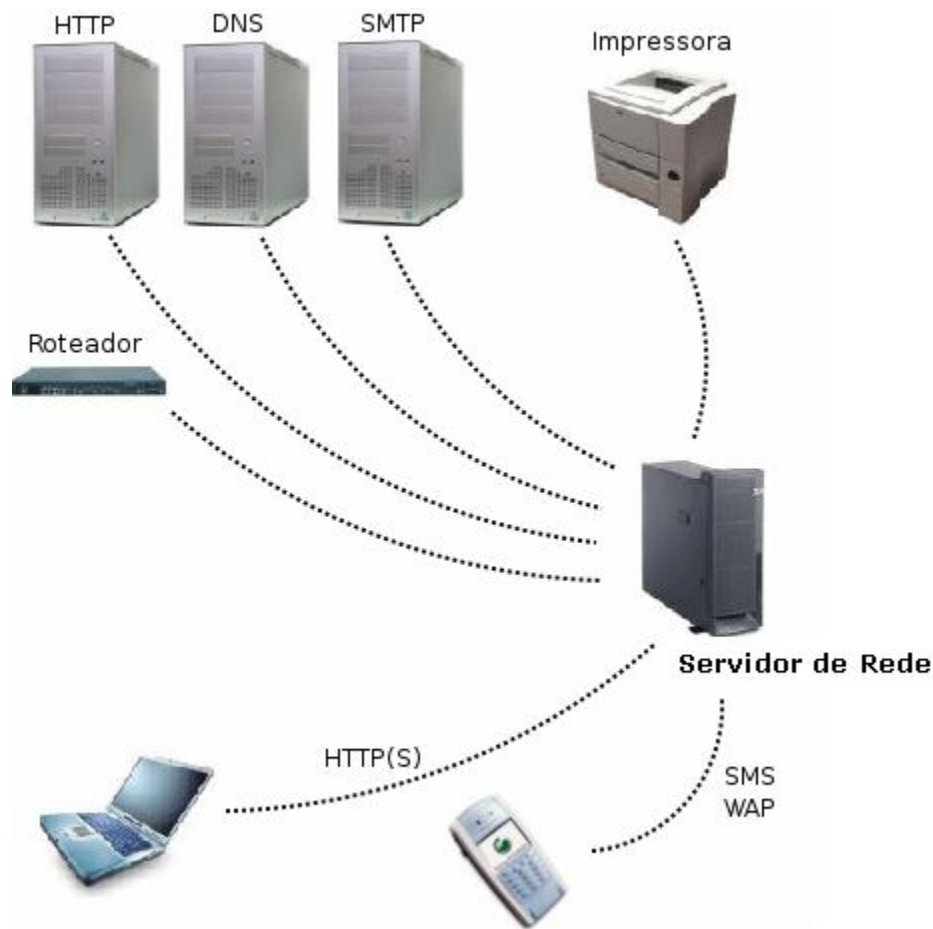
- **Servidor de comunicação**: Conhecidos também como servidores FEP (Front-end Processor), este processador FEP está situado entre o servidor de rede principal, por exemplo, um Mainframe e os usuários da rede. O FEP é responsável pela realização de todos os procedimentos de acesso, interface e comunicação dos usuários com o servidor principal, de forma a permitir o uso dos recursos deste servidor por eles.

- **Servidor Gateway**: São estações da rede que oferecem serviço de comunicação com outras redes para seus clientes. A ligação entre redes pode ser realizada via repetidores ou pontes, mas quando se trata de interligação de redes distintas, isto é,

de arquiteturas diferentes, como, o ir de uma rede de comutação de pacotes para uma rede de comutação de circuitos, ou ainda, o uso de Gateway, nesses casos, se torna indispensável.

- **Servidor Web**: Servidor responsável pelo armazenamento de páginas de um determinado site, requisitados pelos clientes através de Browsers.
- **Servidor de e-mail**: Servidor responsável pelo armazenamento, envio e recebimento de mensagens de correio eletrônico.
- **Servidor de banco de dados**: Servidor que possui e manipula informações contidas em um banco de dados, como, por exemplo, um cadastro de usuários.
- **Servidor DNS**: Servidores responsáveis pela conversão (mapeamento) de endereços de sites em endereços IP e vice-versa. DNS é um acrônimo de Domain Name System, ou sistema de nomes de domínios.
- **Servidor Proxy**: Servidor que atua como um cache, armazenando páginas da internet recém visitadas, aumentando a velocidade de carregamento destas páginas ao chamá-las novamente.
- **Servidor de imagens**: Tipo especial de servidor de banco de dados, especializado em armazenar imagens digitais.
- **Servidor FTP**: Permite acesso de outros usuários a um disco rígido ou Servidor. Esse tipo de servidor armazena arquivos para dar acesso a eles pela internet.
- **Servidor Webmail**: servidor para criar e-mails na Web. Os clientes e os servidores se comunicam através de protocolos, assim como dois ou mais computadores de redes.

Em princípio qualquer computador da nossa rede LAN, se bem configurado, pode atuar em mais de um tipo diferente de servidor. Por exemplo, pode existir em uma rede, um computador que atue como um servidor Web (armazenando as páginas HTML da nossa

empresa) e servidor de banco de dados. Outro computador poderia, por exemplo, atuar como servidor de arquivos, de correio eletrônico e Proxy ao mesmo tempo. Os computadores que agem como um único tipo de servidor são denominados como servidores dedicados. Os servidores dedicados possuem a vantagem de atender a uma requisição de um cliente mais rapidamente.

Um Cluster com três servidores. Com exceção do servidor de banco de dados (um tipo de servidor de aplicação), os demais servidores apenas armazenam informações, ficando por conta do cliente o processamento das informações. No servidor de aplicações, os papéis se invertem, com o cliente recebendo o resultado do processamento de dados da máquina servidora.

Em uma rede heterogênea (com diversos hardwares, softwares) um cliente também pode ser um servidor e assim outro servidor pode ser cliente do mesmo. Por exemplo, uma rede tem

um servidor de impressão e um de arquivos, supondo que você está no servidor de arquivos e necessita imprimir uma folha de um documento que você está escrevendo, quando você mandar imprimir a folha o serviço do servidor de impressão será utilizado, e assim a máquina que você está usando (que é o servidor de arquivos), está sendo cliente do servidor de impressão, pois está utilizando de seu serviço.

Hardware de Servidores

Servidores dedicados, que possuem uma alta requisição de dados por partes dos clientes e que atuam em aplicações críticas utilizam hardware específico para servidores. Já servidores que não possuam essas atuações podem utilizar hardware de um computador comum, não necessitando ser um supercomputador.

Para começar, muitos servidores baseiam-se em entradas e saídas de informações (principalmente gravação e eliminação de arquivos), o que implica em interfaces de entrada e saída e discos rígidos de alto desempenho e confiabilidade. O tipo de disco rígido mais utilizado possui o padrão SCSI (Small Computer System Interface), que permite a interligação de vários periféricos, dispostos em arranjos RAID (Redundant Array of Independent Drives).

Devido a operar com muitas entradas e saídas de informações, os servidores necessitam de processadores de alta velocidade, algumas vezes alguns servidores são multiprocessados, ou seja, possuem mais de um processador.

Em teoria um servidor de rede uma vez em funcionamento nunca deveria ser desligado e permanecer ligado às 24 horas do dia todos os dias, mas isto não é verdade e eles devem ser desligados de tempos em tempos para manutenção. Por ter de operar por muito tempo (de maneira quase ininterrupta), alguns servidores são conectados a geradores elétricos. Outros utilizam sistemas de alimentação, por exemplo, uma fonte de alimentação ininterrupta, também conhecida pelo acrônimo UPS (Uninterruptible Power Supply) que continuam a alimentar o servidor caso haja alguma queda de tensão com o único propósito de não ter perdas de informação.

E, por operar durante longos intervalos de tempos, e devido à existência de um ou mais processadores de alta velocidade, os servidores precisam de um eficiente sistema de dissipação de calor. O que implica em Coolers mais caros, mais barulhentos, porém de maior eficiência e confiabilidade.

Existem outros hardware específicos que podem ser usados como servidores, especialmente placas, do tipo Hot Swapping, que permite a troca destes enquanto o computador está ligado, o que é primordial para que a rede continue a operar.

Discute-se muito sobre a utilização ou não de um micro comum, o popular Personal Computer (PC), como servidor e a necessidade de ou não de se adquirir um equipamento mais robusto para atuar como servidor. A resposta a essa questão depende da utilização do equipamento e do nível crítico do serviço que o servidor está executando. Em uma estrutura não crítica, um computador comum pode ser usado como servidor. Note que o tamanho da rede não importa; por exemplo, uma empresa com 3 instrutores on-line na Internet tem 3 computadores e um deles é o servidor de acesso à Internet. Se este servidor falha o negócio da empresa estaria momentaneamente parado.

Prevendo esse tipo de necessidade, os fabricantes de componentes de computadores desenvolvem placas mais robustas, aplicam uma engenharia mais elaborada de ventilação, redundância de itens e capacidade de expansão ampliada, para que o servidor possa garantir a disponibilidade do serviço e a confiabilidade no mesmo. Normalmente a

preocupação em desenvolver servidores fica centrada em grandes fabricantes do mercado, que possuem equipes preparadas e laboratórios com esse fim.

Software de Servidores

Para que funcione uma rede cliente servidor, é necessário que no servidor esteja instalado um sistema operacional que reconheça esse tipo de rede. Os sistemas operacionais para redes do tipo Cliente/Servidor são:

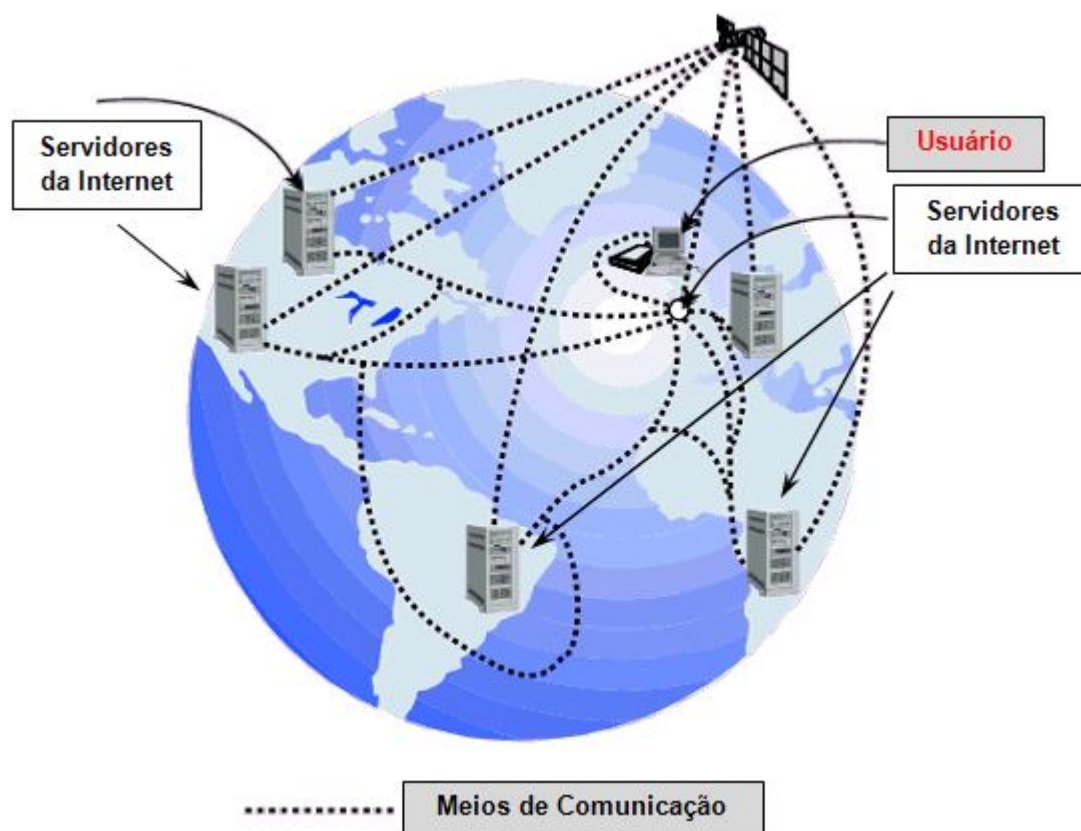
- Windows NT, Windows 2000, Windows 2003R2, Windows Server 2008.
- Todas as versões de Unix:
  - AIX da IBM
  - IRIX da SGI
  - Solaris da SUN
  - HPux da HP
  - Ultrix da Digital
  - True64 da DEC
  - Linux
  - FreeBSD
  - MacOS X
- Novell Netware (já quase em deuso).

Os sistemas operacionais Windows 95, Windows 98 e Windows ME reconhecem somente redes do tipo Ponto-a-Ponto (Peer-to-Peer); e o sistema operacional DOS não tem suporte a

qualquer tipo de rede. Em servidores, o sistema Unix e sistemas baseados neste, tais como Linux, Solaris, FreeBSD, XFree86, etc., são os sistemas mais utilizados, ao passo que os sistemas Windows, são bem menos utilizados.

Servidores na Internet

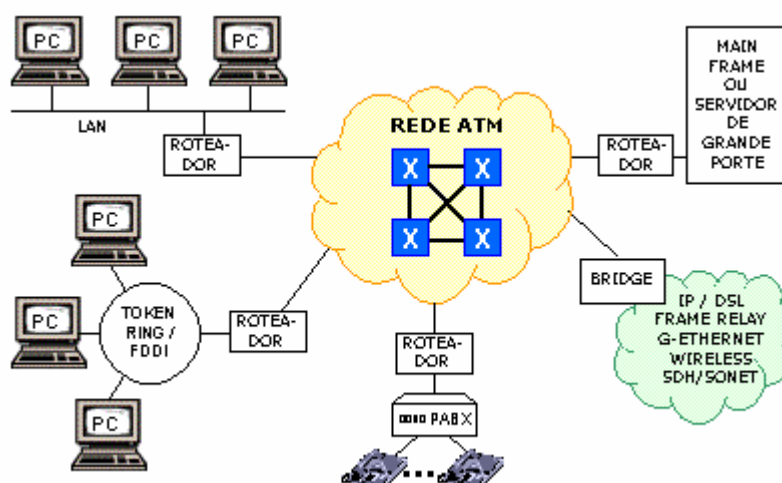
A Internet, atualmente a maior rede de computadores do mundo, utiliza o modelo cliente-servidor. Muitos servidores em todo o mundo são interligados e processam informações simultaneamente.

Alguns serviços oferecidos por servidores da Internet são: páginas Web, correio eletrônico, transferência de arquivos, acesso remoto, mensagens instantâneas, motores de busca e outros. É interessante notar que qualquer ação efetuada por um usuário envolve o trabalho de diversos servidores espalhados pelo mundo todo e conectados através de diferentes tipos de meios de comunicação.

UNIDADE 22

Objetivo: Saber o que é, qual a utilidade e como funciona uma rede ATM.

Tecnologias de Redes (Parte I)

Tecnologia ATM

A tecnologia ATM (Asynchronous Transfer Mode), ou seja, o Modo de Transmissão Assíncrono é uma forma de tecnologia baseada na transmissão de pequenos blocos de dados de tamanho fixo e estrutura definida denominados células ATM (ATM cells). Estas células são transmitidas através de conexões de circuitos virtuais estabelecidos, sendo sua entrega e comutação feitas pela rede baseado na informação de seu cabeçalho. Esta tecnologia se adapta facilmente às exigências de uma grande gama de tráfegos, suportando com isto diferente tipos de serviços. Com isto, a tecnologia ATM foi escolhida de forma a dar suporte à implantação da Rede Digital de Serviços Integrados - Faixa Larga RDSI-FL ou pelas siglas em inglês Broadband-Integrated Services Digital Network (B-ISDN).

Não há como se falar de redes ATM sem se ater por alguns momentos em redes RDSI-FL. Na verdade a história e evolução das redes ATM, bem como a sua normalização através das

recomendações do CCITT (atual ITU-T), aconteceram dentro do contexto da evolução da Rede Digital de Serviços Integrados - Faixa Larga.

O ATM é uma tecnologia de comunicação de dados de alta velocidade usada para interligar redes locais, metropolitanas e de longa distância para aplicações de dados, voz, áudio, e vídeo.

Basicamente a tecnologia ATM fornece um meio para enviar informações em modo assíncrono através de uma rede de dados, dividindo essas informações em blocos de dados de tamanho fixo, estes blocos são denominados células ATM (ATM cells). Cada célula carrega um endereço que é usado pelos equipamentos da rede para determinar o seu destino.

A tecnologia ATM utiliza o processo de comutação de pacotes, que é adequado para o envio assíncrono de informações com diferentes requisitos de tempo e funcionalidades, aproveitando-se de sua confiabilidade, eficiência no uso de banda e suporte a aplicações que requerem classes de qualidade de serviço diferenciadas.

Evolução da Tecnologia ATM

Os trabalhos de padronização sobre a RDSI-FL foram iniciados pelo BBTG (Broad Band Task Group) do SG18 do ITU-T, no começo do oitavo período de estudos (1985-1988). A primeira recomendação aprovada veio em 1988, incluindo a adoção do ATM como o modo de transferência para suporte à Rede Digital de Serviços Integrados - Faixa Larga. Ao todo, doze recomendações foram aprovadas no encontro de Matsuyama (novembro/1990) que definem os serviços oferecidos, a arquitetura em camadas para redes ATM, as camadas desta rede, os princípios de funcionamento de uma rede ATM, bem como os aspectos relacionados à sua operação e manutenção. Algumas recomendações surgiram no período de estudos atual (1993-1996), como a I.374 que traz as especificações das características necessárias para a que a rede RDSI-FL ofereça suporte a serviços multimídia.

Portanto, no fim da década de 80 e início da década de 90, vários fatores combinados demandaram a transmissão de dados com velocidades mais altas:

- A evolução das redes transmissão para a tecnologia digital em meios elétricos, ópticos e rádio;
- A descentralização das redes e o uso de aplicações cliente / servidor;
- A migração das interfaces de texto para interfaces gráficas;
- O aumento do tráfego do tipo rajada (Bursty) nas aplicações de dados e o consequente aumento do uso de banda;
- O aumento da capacidade de processamento dos equipamentos de usuário (PCs, estações de trabalho, terminais Unix, entre outros);
- A demanda por protocolos mais confiáveis e com serviços mais abrangentes.

Nessa época, consolidava-se o desenvolvimento das tecnologias ISDN e Frame Relay. Entretanto, a crescente necessidade de maior uso de banda e de classes de serviços diferenciadas, de acordo com o tipo de aplicação, levou ao desenvolvimento das tecnologias ATM e B-ISDN, com padrões e recomendações elaborados por órgãos internacionais de Telecomunicações, tais como o CCITT (atual ITU) e suportados pela indústria mundial.

Uma rede ATM é composta por:

- Equipamentos de usuários (PCs, estações de trabalho, servidores, computadores de grande porte, PABX, etc.) e suas respectivas aplicações;
- Equipamentos de acesso com interface ATM (roteadores de acesso, Hubs, Switches, Bridges, etc.);
- Equipamentos de rede (Switches, roteadores de rede, equipamentos de transmissão com canais E1 / T1 ou de maior banda, etc.).

A conversão dos dados para o protocolo ATM é feita pelos equipamentos de acesso. Os Frames gerados são enviados aos equipamentos de rede, cuja função é basicamente transportar esses Frames até o seu destino, usando os procedimentos de roteamento próprios do protocolo.

A rede ATM é sempre representada por uma nuvem, já que ela não é uma simples conexão física entre 2 pontos distintos. A conexão entre esses pontos é feita através de rotas ou canais virtuais VP/VC (Virtual Path/Virtual Channel) configurados com uma determinada banda. A alocação de banda física na rede é feita pelo tipo de serviço requisitado à rede ATM para o envio de tráfego (vídeo, voz, dados) que será transportado pelas células.

VPI / VCI (Virtual Path Identifier / Virtual Circuit Identifier)

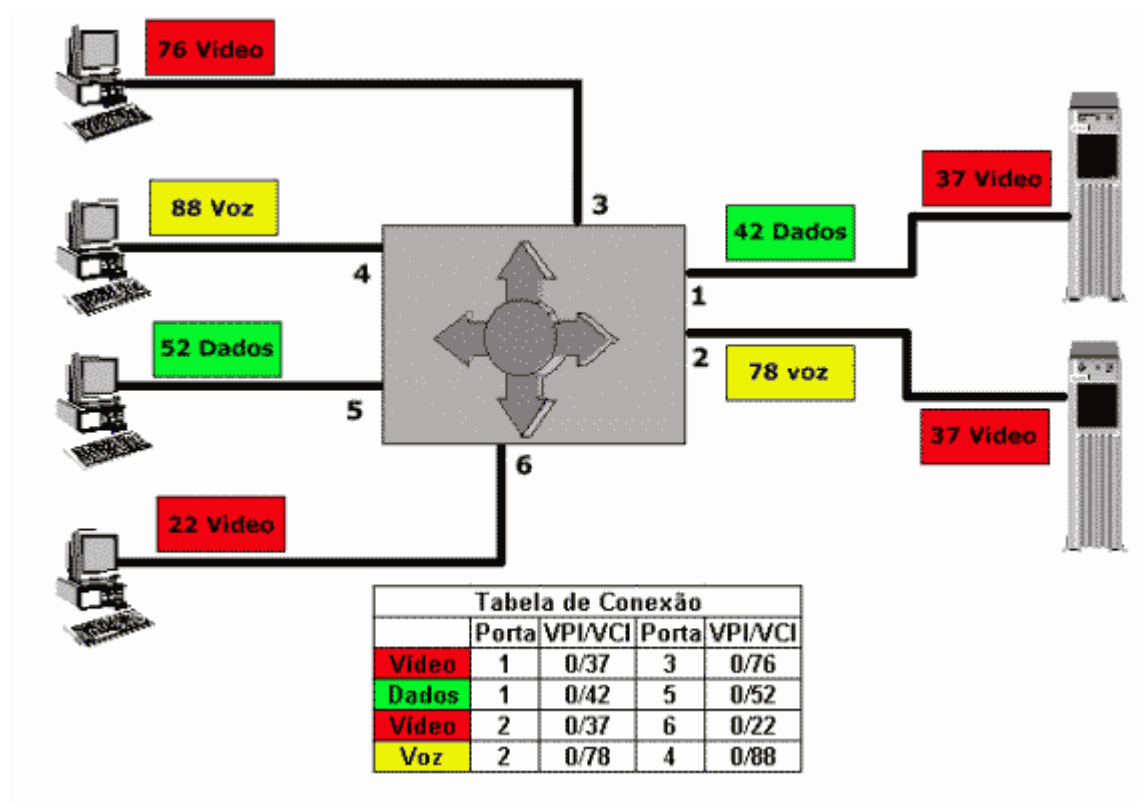
A conexão com a rede ATM é identificada por dois indicadores, Identificador de Caminho Virtual (VPI) e Identificador do Circuito Virtual (VCI). Cada conexão deve ter uma configuração de VPI/VCI exclusiva. Por exemplo: VPI-8 VCI-35.

VPI/VCI - As portas no modem ADSL, são descritas como virtuais porque ela é associada à rede ATM, neste caso para configurar os VCI/VPI, o usuário deverá entrar em contato com seu provedor de serviços ADSL. O modem ADSL no modo Bridge é configurado com os seguintes parâmetros:

- **VPI**: Caminho virtual de identificação.
- **VCI**: Circuito virtual de identificação.
- **LLC (Logical Link Control)**: Controle lógico de ligação permite múltiplos protocolos.
- **VC-MUX (Virtual Circuit-Multiplexing) (Null Encapsulation)**: Permite somente um único tipo de tráfego, ou seja, o tráfego que será enviado pelo circuito virtual terá um único protocolo, isto evita a sobrecarga de processamento (Overhead) nos comutadores ATM. Como só um tipo de tráfego será enviado não existe informação adicional agregada às células daí o nome de encapsulamento nulo.

- **Habilitando NAPT (Network Address Port Translation)**: Esta opção funciona unicamente para um modem ADSL configurado em modo roteador, portanto, não pode ser utilizado em modo Bridge ou PPP.

Os campos responsáveis situados no cabeçalho em levar a célula de um ponto a outro são o VPI (Virtual Path Identifier) e o VCI (Virtual Channel Identifier) respectivamente, como mostrado no exemplo abaixo de um número de conexões virtuais através de um switch ATM. Dentro de um switch existe uma tabela de roteamento (Routing Table) que associa um campo VCI/VPI e uma porta a outra porta e a outro VCI/VPI.

Tabela de Conexão				
	Porta	VPI/VCI	Porta	VPI/VCI
Video	1	0/37	3	0/76
Dados	1	0/42	5	0/52
Video	2	0/37	6	0/22
Voz	2	0/78	4	0/88

Quando uma célula chega ao Switch, este verifica o valor do VCI/VPI, por exemplo, 0/37. Como a célula veio pela porta 1, o Switch determina que deve sair pela porta 3. E, além disso, o VCI/VPI é alterado para 0/76. A célula apenas passa pelo Switch, mudando apenas um campo do cabeçalho, não alterando o conteúdo de sua informação.

Os valores VPI/VCI mudam por dois motivos. Primeiro, se os valores fossem únicos existiriam aproximadamente 17 milhões de valores diferentes disponíveis. Como a rede é muito grande, 17 milhões não seriam suficientes para representar todo o tráfego de células. O segundo é devido à administração de valores únicos em uma rede tão imensa como a Internet. É impraticável comparar a conexão que você está para fazer com a do resto do mundo para saber se alguém a está usando!

Os valores de VCI/VPI têm significado apenas em uma dada interface. De fato, neste exemplo, 37 foi usado nas duas interfaces, mas não há risco de ambiguidade estão em interfaces físicas distintas. A combinação dos campos VCI/VPI permite associar uma dada célula a uma dada conexão, e assim, a célula pode ser encaminhada corretamente ao seu destino.

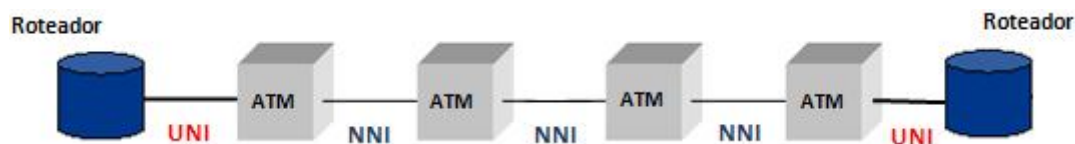
A tabela abaixo apresenta a relação de VPI e VCI utilizados atualmente pelas principais operadoras de telefonia fixa, para o serviço ADSL, no Brasil.

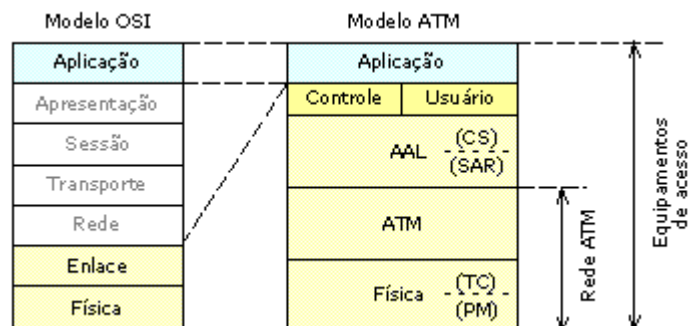
Organização	VPI	VCI
Speedy (Telefônica)	8	35
Velox (Telemar)	0	33
Brasil Telecom	0	35
Brasil Telecom (RS)	1	32
CTBC	0	35
TurboNet (GVT)	1	35

Características Da Tecnologia ATM

A tecnologia ATM utiliza a multiplexação e comutação de pacotes para prover um serviço de transferência de dados orientado a conexão, em modo assíncrono, para atender as necessidades de diversos tipos de aplicações de dados, voz, áudio e vídeo.

Diferentemente dos protocolos X.25 e Frame Relay, entre outros, o ATM utiliza um pacote de dados de tamanho fixo denominado célula. Uma célula possui 53 bytes, sendo 48 para a informação útil e 5 para o cabeçalho. Cada célula ATM enviada para a rede contém uma informação de endereçamento que estabelece uma conexão virtual entre origem e destino. Este procedimento permite ao protocolo implementar as características de multiplexação estatística e de compartilhamento de portas. Na tecnologia ATM as conexões de rede são de 2 tipos:

1. **UNI (User-to-Network Interface)**: É a conexão entre equipamentos de acesso (por exemplo, roteadores) e um comutador ATM, isto se aplica aos comutadores ATM que se encontram nas bordas da rede.
2. **NNI (Network-to-Network Interface)**: É a forma de conexão entre os comutadores internos da rede ATM.

No primeiro caso, informações de tipo de serviço são relevantes para a forma como estes serão tratados pela rede, e referem-se a conexões entre usuários finais. No segundo caso, o controle de tráfego é função única e exclusiva das conexões virtuais configuradas entre os comutadores ATM. O protocolo ATM foi concebido através de uma estrutura em camadas, porém sem a pretensão de atender ao modelo OSI.

A figura abaixo apresenta sua estrutura e compara com o modelo OSI.

No modelo ATM todas as camadas possuem funcionalidades de controle e de usuário (serviços), conforme apresentado na figura acima. A descrição de cada camada ATM é apresentada a seguir:

- **AAL (ATM Adaptation Layer)**: É responsável pelo fornecimento de serviços para a camada de aplicação superior. A subcamada CS (Convergence Sublayer) converte e prepara a informação de usuário para o ATM, de acordo com o tipo de serviço, além de controlar as conexões virtuais. A subcamada SAR (Segmentation and Reassembly) fragmenta a informação para ser encapsulada na célula ATM. A camada AAL implementa ainda os respectivos mecanismos de controle, sinalização e qualidade de serviço. Dependendo do tipo de tráfego (Dados, Voz ou Vídeo) a rede ATM fornecerá um tipo de serviço, cada serviço faz uso de um dos seguintes tipos de Adaptation Layers:
    - **AAL1**: Para tráfego orientado à conexão apresentando uma taxa de bit constante CBR (Constant Bit Rate). Exemplos deste serviço incluem canais de voz digitalizada a 64 Kbps, emissão de vídeo (não compactado) com taxa fixa e linhas alugadas para redes de dados privadas.
    - **AAL2**: Para tráfego orientado à conexão com uma taxa de bit variável VBR (Variable Bit Rate), este serviço requer de certos limites de atraso para o envio do tráfego. Exemplos deste serviço incluem voz ou vídeo compactado. O

requerimento de limites sobre o atraso é necessário para que o receptor possa reconstruir o vídeo ou voz original descompactada.

- **AAL3/4**: Para tráfego orientado à conexão. Duas AAL foram definidas para atender este tipo de tráfego, e foram juntadas em uma só conhecida como a AAL3/4. Devido a sua complexidade, a AAL5 é (às vezes) utilizada também para este tipo de tráfego. As aplicações utilizam o que se conhece como a taxa de bit disponível ABR (Available Bit Rate), por exemplo, transferência de arquivos ou aplicações de rede em geral onde a conexão deve ser estabelecida (negociar com a rede ATM) antes de iniciar a transferência de dados, embora se tenha certa qualidade de serviço, não sem tem restrições nos limites de atrasos para o envio das células.

- **AAL5**: Para tráfego não orientado à conexão. Exemplos deste serviço incluem tráfego Internet, aplicações de rede em geral onde não se têm nenhum tipo de configuração (negociação) inicial da conexão, para com a rede ATM, antes de transmitir os dados. Para este tipo de aplicações tanto a AAL3/4 ou a AAL5 podem ser utilizadas. Neste caso como as aplicações de rede não fazem nenhuma negociação (ou configuração) previa com a rede, são conhecidas como aplicações (ou tráfego) que utilizam uma taxa de bit não especificada UBR (Unspecified Bit Rate), a capacidade do canal que estiver livre será utilizada por estas aplicações.

- **ATM**: É responsável pela construção, processamento e transmissão das células, e pelo processamento das conexões virtuais. Esta camada também processa os diferentes tipos e classes de serviços e controla o tráfego da rede. Nos equipamentos de rede esta camada trata todo o tráfego de entrada e saída, minimizando o processamento e aumentando a eficiência do protocolo sem necessitar de outras camadas superiores.

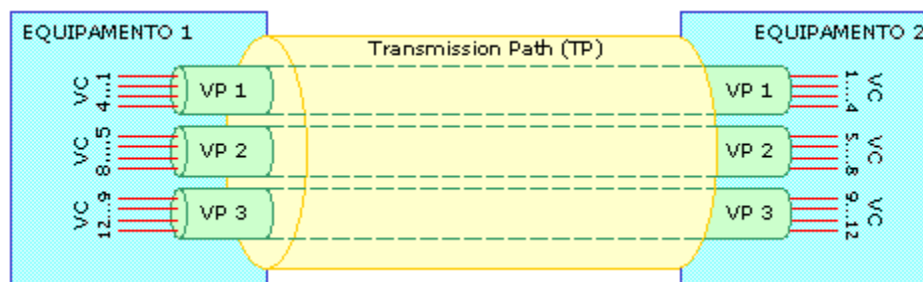
- **Física**: Provê os meios para transmitir as células ATM. A subcamada TC (Transmission Convergence) mapeia as células ATM no formato dos frames da rede

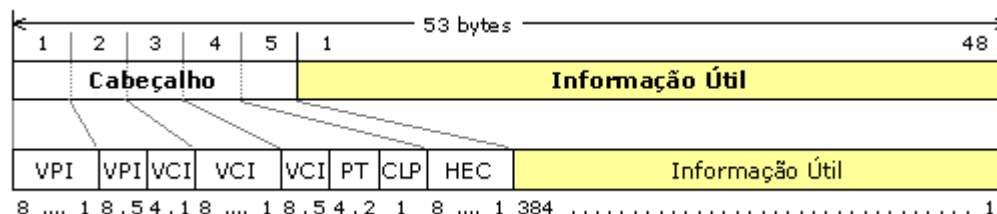
de transmissão (SDH, SONET, PDH, etc.). A subcamada PM (Physical Medium) temporiza os bits do frame de acordo com o relógio de transmissão.

A seguir são apresentados as conexões virtuais, a célula ATM e os tipos de serviços oferecidos pelas redes ATM.

Conexões Virtuais ATM

A tecnologia ATM é baseada no uso de conexões virtuais. O ATM implementa essas conexões virtuais usando 3 conceitos:

- **TP (Transmission Path)**: É a rota de transmissão física (por exemplo, circuitos das redes de transmissão SDH/SONET) entre 2 equipamentos da rede ATM.
- **VP (Virtual Path)**: É a rota virtual configurada entre 2 equipamentos adjacentes da rede ATM. O VP usa como infraestrutura os TP's. Um TP pode ter um ou mais VP's. Cada VP tem um identificador VPI (Virtual Paths Identifier), que deve ser único para um dado TP.
- **VC (Virtual Channel)**: É o canal virtual configurado também entre 2 equipamentos adjacentes da rede ATM. O VC usa como infraestrutura o VP. Um VP pode ter um ou mais VC's, Cada VC tem um identificador VCI (Virtual Channel Identifier), que também deve ser único para um dado TP.

Estrutura Da Célula ATM

Uma célula ATM utiliza a estrutura simplificada com tamanho fixo de 53 Bytes (5 Bytes de cabeçalho mais 48 Bytes para dados de usuário) apresentada na figura a seguir.

O campo de Cabeçalho carrega as informações de controle do protocolo. Devido a sua importância, possui mecanismo de detecção e correção de erros para preservar o seu conteúdo. Ele é composto por 5 Bytes com as seguintes informações:

1. **VPI (Virtual Path Identifier)**: Com 12 bits, representa o número da rota virtual até o destinatário da informação útil, e tem significado local apenas para a porta de origem. Nas conexões UNI o VPI pode ainda ser dividido em 2 campos: o GFC (Generic Flow Control), com 4 bits, que identifica o tipo de célula para a rede, e o VPI propriamente dito, com 8 bits.

2. **VCI (Virtual Channel Identifier)**: Com 16 bits, representa o número do canal virtual dentro de uma rota virtual específica. Também se refere ao destinatário da informação útil e tem significado local apenas para a porta de origem.

3. **PT (Payload Type)**: Com 3 bits, identifica o tipo de informação que a célula contém: de usuário, de sinalização ou de manutenção.

4. **CLP (Cell Loss Priority)**: Com 1 bit, indica a prioridade relativa da célula. Células de menor prioridade são descartadas antes que as células de maior prioridade durante períodos de congestionamento.

5. **HEC (Header Error Check)**: Com 8 bits, é usado para detectar e corrigir erros no cabeçalho.

O campo de Informação Útil, com 384 bits (48 Bytes) carrega as informações de usuário ou de controle do protocolo. A informação útil é mantida intacta ao longo de toda a rede, sem verificação ou correção de erros. A camada ATM do protocolo considera que essas tarefas são executadas pelos protocolos das aplicações de usuário ou pelos processos de sinalização e gerenciamento do próprio protocolo para garantir a integridade desses dados.

Quando é informação de usuário, o conteúdo desse campo é obtido a partir da fragmentação da informação original executada na camada AAL de acordo com o serviço. O campo pode ainda servir de preenchimento nulo, nos casos de serviços da taxa constante de bits. Quando a informação é de controle do protocolo, o primeiro byte é usado como campo de controle e os demais bytes contem informação de sinalização, configuração e gerenciamento da rede.

Categorias De Serviço ATM

Uma categoria de serviço ATM tem como objetivo traduzir um modelo de serviço, isto é, uma combinação de caracterização de tráfego e requisitos de qualidade de serviço (QoS) em um conjunto de procedimentos de caracterização de tráfego e gerenciamento de recursos que sejam adequados para um tipo de serviço, permitindo desta forma a alocação eficiente de recursos pela rede.

O ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) e o ATM Forum apresentam algumas distinções importantes quanto aos nomes e tipos de categorias. O ITU-T define quatro diferentes categorias, a saber:

- DBR (deterministic bit rate);
- SBR (statistical bit rate);

- ABT (ATM block transfer); e
- ABR (available bit rate).

Já o ATM Forum faz uma divisão em cinco categorias:

1. **CBR (Constant Bit Rate)**: O CBR é aplicado em conexões que necessitam de banda fixa (estática) devido aos requisitos de tempo bastante apertados entre a origem e o destino. Aplicações típicas deste serviço são: áudio interativo (telefonia), distribuição de áudio e vídeo (televisão, pay-per-view, etc), áudio e vídeo on demand, e emulação de circuitos TDM.

2. **VBR (Variable Bit Rate) real-time**: O serviço VBR em tempo real (VBR-rt), é aplicado às conexões que têm requisitos apertados de tempo entre origem e destino, porém a taxa de bits pode variar. Aplicações típicas deste serviço são: tráfego de voz (telefonia) com taxa de bit variável e vídeo comprimido (MPEG, por exemplo).

3. **VBR (Variable Bit Rate) nonreal-time**: O serviço VBR em tempo não real (VBR-nrt) pode ser utilizado com ou sem conexão, e destina-se às conexões que, embora críticas e com requisitos de tempo apertados, podem aceitar variações na taxa de bits. Aplicações típicas deste serviço são os sistemas de vídeo sobre demanda (Vídeo On-Demand), reserva de passagens aéreas, Home Banking, emulação de LAN para a interligação de redes com protocolos diversos (por exemplo, interação com redes Frame Relay, etc.).

4. **ABR (Available Bit Rate)**: Este serviço de taxa de bit disponível é aplicado às conexões que transportam tráfego em rajadas que podem prescindir da garantia de banda, variando a taxa de bits de acordo com a disponibilidade de banda da rede ATM. Aplicações típicas deste serviço também são as interligações entre redes (com protocolo TCP/IP, entre outros) e a emulação de LANs onde os equipamentos de interfaces têm funcionalidades ATM.

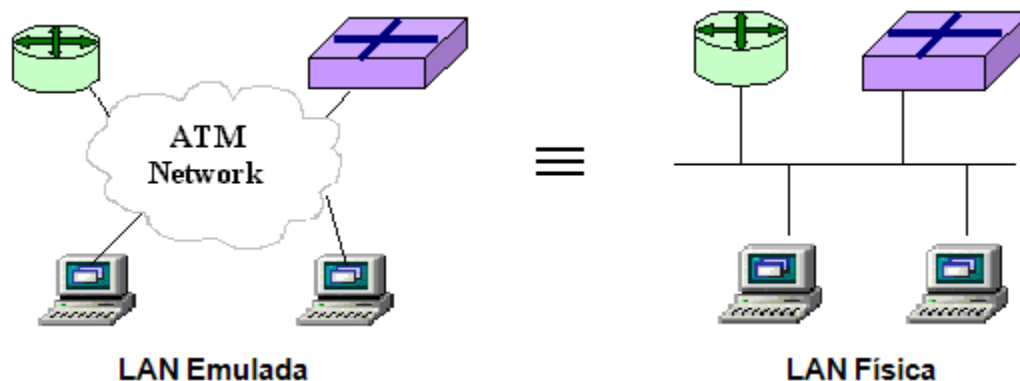
5. **UBR (Unspecified Bit Rate)**: O serviço UBR é aplicado às conexões que transportam tráfego que não tem requisitos de tempo real e cujos requisitos e atrasos ou variações destes atrasos são mais flexíveis. Aplicações típicas deste serviço também são as interligações entre redes e a emulação de LANs que executam a transferência de arquivos e e-mails.

Como a tecnologia ATM deve coexistir com as tecnologias (muito bem estabelecidas) de redes LAN, tais como, Ethernet (em muito uso atualmente), Token-Ring (quase inexistente), etc. É extremamente essencial que exista uma suave harmonia entre todas elas. Nesse sentido, o ATM Fórum junto com a ITU-T indicam métodos e ferramentas que possam fazer uma boa interface entre tecnologias LAN e a tecnologia ATM, nesse sentido, surgiu o conceito de emulação de LAN ou LAN emulada (LAN Emulation).

LAN Emulation (LANE)

Há duas palavras muito parecidas, mas com significados bem diferentes. Simulação e Emulação. A simulação tem a ver com o fato de imitar algo, fazer de conta. É o de apresentar uma aparência exterior bem diferente da interior, de modo que quem olha para o objeto a ser simulado não o distingue de outro idêntico. Um objeto é real, e o outro apenas o é na sua aparência. Por exemplo, simular uma pessoa é tentar imitar a sua voz, andar, tiques, perfil, etc.

Por outro lado, a emulação consiste em transformar um objeto em outro naquilo que esse tem de fundamental, é um esforço por igualar, mas permanecendo diferente. Por exemplo, emular uma pessoa é tentar pensar como ela pensa, sentir como sente, transformar-se na outra pessoa, contudo sem qualquer tipo de preocupação na imitação de voz, perfil, ou outro aspecto exterior.

Portanto, para emular uma rede LAN a rede ATM deve garantir que as características principais de comportamento de uma rede LAN estejam disponíveis nas interfaces de rede ATM que se conectam com as LANs, ou seja, a rede ATM continuará sendo uma rede ATM sem perder as características próprias dela, porém algumas características de redes LAN, no nível de enlace de dados (camada 2 do modelo OSI), serão introduzidas nela para que exista uma boa interface entre as LANs e a rede ATM, isso basicamente é o LANE (LAN Emulation).

O protocolo ATM não impõe limitações físicas quanto a distâncias, como também não impõe limites na largura de banda a ser disponibilizada, pois, o tráfego de dados se dá Ponto-a-Ponto entre as estações por meio de circuitos virtuais e os links ATM podem rodar a uma velocidade de 622 Mbps ou mais. Assim, uma rede local sobre ATM permitiria a implementação de segmentos de redes que excederiam as limitações de redes reais em termos de alcance físico, largura de banda e número de estações.

Entretanto, este aproveitamento ficou condicionado à capacidade das redes ATM de interoperar com as redes locais de computadores uma vez que nem todas as aplicações para LAN são providas por redes ATM e dificilmente um usuário iria investir no projeto de uma rede que não fosse capaz de se comunicar com toda a base instalada.

Dentro deste contexto e procurando solucionar essa questão de interoperabilidade, foi criado o LAN Emulation (LANE), um conjunto de especificações técnicas desenvolvidas pelo ATM Fórum para redes ATM, que emula os serviços existentes em redes Ethernet (802.3) e

Token-Ring (802.5), permitindo aos usuários de LANs comuns usufruírem (de quase todas) as vantagens das redes ATM sem necessitar de modificações na estrutura do hardware ou do software das estações de rede local.

O Conceito De LANE

LANE é um serviço implementado através de uma camada de software em qualquer estação que possua uma interface ATM, seja ela um computador, Switch ou roteador. Sua função básica é oferecer ao protocolo da camada rede uma interface idêntica à oferecida por uma rede local tradicional, ou seja, uma LANE suporta a transmissão de quadros Ethernet e Token-Ring sobre redes ATM de modo que, a princípio, não se façam necessárias modificações nas redes já existentes para operar uma rede local ATM. Assim, a LANE habilita uma rede ATM a agir como Backbone LAN para Hubs, LAN Switches, Bridges e roteadores.

Portanto, uma LANE é o padrão do ATM Fórum para dar suporte à interconexão das redes LAN tradicionais, emulando os protocolos MAC das redes Token-Ring e Ethernet através de uma rede ATM. O conceito de LANE define uma rede VLAN (Virtual LAN) que consiste de várias redes LAN e um segmento ELAN (Emulated LAN) que é a própria rede ATM. Roteadores podem conectar múltiplas VLANs. A LANE fornece todas as características aos dispositivos LECs que são os encarregados de se comunicar com os serviços de LECS, LES e BUS através da ELAN (ou seja, da rede ATM).

Basicamente o conceito de LANE = ELAN + LANs, onde ELAN é a própria rede ATM que se apresenta exatamente como se fosse uma rede Ethernet ou Token-Ring aos computadores e às aplicações que funcionam nas LANs, mas a LANE (na verdade) implementa todas as funcionalidades e vantagens de uma rede ATM. Nesse sentido as redes virtuais VLAN utilizando o padrão LANE seriam um recurso ótimo para aquelas empresas que tenham redes LANs espalhadas geograficamente.

Cada roteador (ou Switch) de LAN requer de uma interfase ATM, muito bem configurada, que suporte a emulação LAN, essa interfase será a responsável por traduzir os endereços MAC em endereços ATM e abrir uma conexão entre dois pontos finais. Com isto, não há necessidade de nenhuma mudança de protocolos e de aplicações na rede LAN instalada já que os Drivers (Software) de rede fornecem interfaces idênticas, isto é, o NDIS (Network Driver Interface Specification) será igual aos níveis superiores da rede. Em princípio, basta ligar um HUB LANE, instalar uma placa de conexão à rede, carregar os Drivers fornecidos pelo fabricante e já se terá uma interface ATM LANE na rede local.

Com o exposto anteriormente pode-se definir os seguintes conceitos importantes sobre o padrão LANE do ATM Forum:

1. **ELAN (Emulated LAN)**: É a parte (ou segmento) ATM de uma VLAN baseada no padrão LANE. Portanto, uma VLAN consiste de um segmento ELAN (que é a própria rede ATM) que interconecta segmentos (ou redes) LAN tradicionais.

2. **VLAN (Virtual LAN)**: É uma arquitetura (ou infraestrutura) de rede a qual permite que usuários geograficamente distribuídos se comuniquem como se estivessem numa única rede LAN física, ou seja, compartilhando um mesmo domínio de broadcast e multicast.

Utilização Do LANE

O conceito LANE utiliza redes ATM como Backbone para interligar as LANs existentes, criando uma camada de conversão que mascara a conexão ATM para as aplicações que requerem uma transferência de dados sem conexão. Permite a implementação de um conjunto de dispositivos que implementam uma aplicação de rede local emulada (ELAN) analogamente a um grupo de estações LAN ligadas a uma rede Ethernet ou Token-Ring, nesse caso, sobre uma rede ATM. Dessa forma, uma ELAN provê a transmissão de quadros (Frames) de dados entre seus usuários, de maneira semelhante a uma LAN física.

Podem-se ter várias ELANs em uma mesma rede ATM física, mas estas ELANs são logicamente independentes. Lembrar que a ELAN é a parte da LANE que representa à rede ATM, agora uma única rede ATM (agindo como Backbone) pode suportar várias redes LAN de diferentes corporações, isto é, cada corporação terá sua própria ELAN dentro de uma mesma infra-estrutura de rede ATM.

Por exemplo, em uma cidade de grande porte varias instituições podem fazer uso de VLANs utilizando a mesma infra-estrutura da rede ATM física que a empresa de telecomunicações pública oferece, mas estas VLANs seriam logicamente independentes umas das outras. Basta configurar LANEs para cada corporação com caminhos e canais virtuais diferentes. Desta forma é possível verificar a existência de várias ELANs dentro de uma mesma rede ATM física, sendo todas elas logicamente independentes umas das outras.

Componentes De Uma LANE

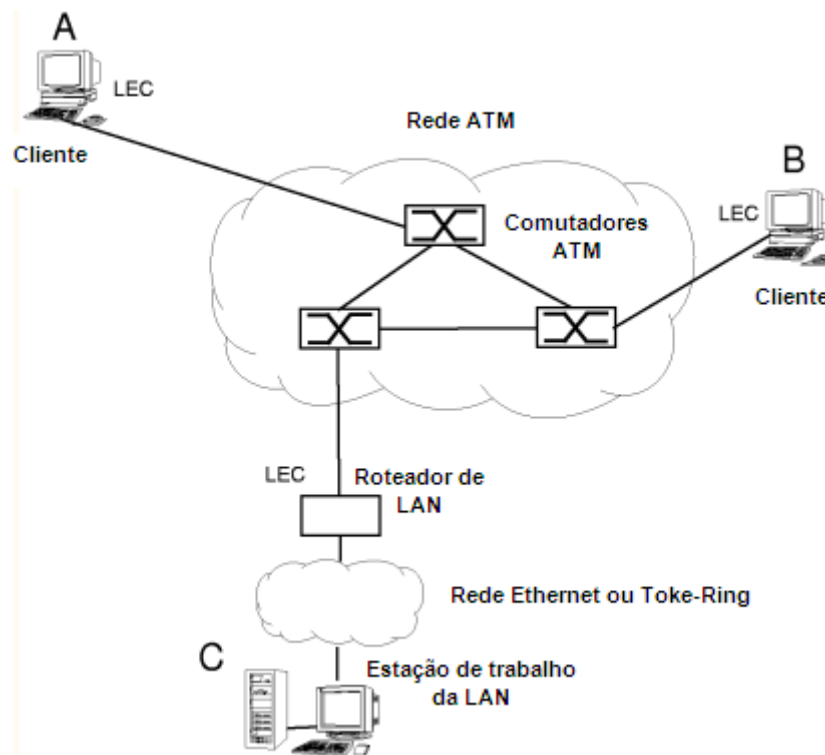
Existem dois tipos de LANE: Ethernet e Token-Ring. Ambas são compostas por um conjunto de LECs (LAN Emulation Clients) e pelo serviço, que consiste de três servidores distintos: o LECS (LANE Configuration Server), o LES (LANE Server) e o BUS (Broadcast & Unknown Server).

A interface entre os clientes e o serviço é definida pelo protocolo LUNI (LAN Emulation User to Network Interface), que é o objeto da norma de LAN Emulation. A interface entre os elementos do serviço está definida na norma LNNI (LANE Network Node Interface):

1. **LAN Emulation Client (LEC)** – Uma entidade numa extremidade como, por exemplo, uma workstation, LAN switch ou roteador que realiza a transmissão e recepção, endereçamento e outras funções de controle para um único terminal numa única ELAN. O cliente da LANE provê serviços LAN para as camadas superiores que fazem a interfase com ele. Um roteador pode ter múltiplos clientes LANE um para cada interfase de rede LAN, e em alguns casos cada um conectado a diferentes ELANs;

2. **LANE Configuration Server (LECS)** – Um servidor que designa clientes individuais a determinadas ELANs direcionando-os aos LES correspondentes das ELANs. O LECS mantém um banco de dados dos clientes LANE (ou dos endereços MAC) e suas ELANs. O LECS pode ser usado para segurança restringindo a associação de ELANs a certos LECs baseados nos seus endereços MAC;

3. **LANE Server (LES)** – Um servidor que provê uma facilidade de registro para os clientes ao se juntar a uma ELAN. Cada ELAN tem um LES que trata dos protocolos de pedidos de resolução de endereço de LANE, o que é uma tabela (Look-up Table) de endereços MAC de destino;

4. **Broadcast & Unknown Server (BUS)** – Um servidor que trata do tráfego com destino desconhecido, de Multicast e Broadcast para os clientes sem uma ELAN.

Qual A Importância Da LANE?

Esse conceito foi desenvolvido porque a tecnologia ATM deve coexistir com tecnologias de rede LAN bem estabelecidas como ser: Ethernet, Token-Ring. Nesse sentido, o ATM Forum definiu o conceito de LANE para permitir, aos usuários de LANs comuns, usufruir das vantagens das redes ATM sem ter a necessidade de fazer modificações no hardware ou software de suas estações terminais de rede LAN.

Uma razão para a utilização de LANE é que algumas das aplicações atuais para LANs não são providas por redes ATM. A grande maioria das aplicações para LANs assume que são capazes de:

- Distribuir os datagramas para destinos individuais de acordo com um único endereço MAC, sem nenhum tipo de conexão real com aquele endereço.
- Distribuir pacotes para todos os usuários participantes da rede (Broadcast) ou para um grupo específico de usuários (Multicast) através de um endereço MAC especial indicando Broadcast ou Multicast.

As redes ATM não oferecem nenhum destes serviços diretamente. Como explicado anteriormente, as redes ATM distribuem datagramas em canais de conexão virtual (Virtual Channel) que necessitam ser estabelecidos entre as extremidades interessadas antes do início do envio dos pacotes.

Uma rede ATM requer conexões ponto-multiponto para que se possibilite o envio de pacotes Broadcast ou Multicast. Logo as redes ATM implementam conexões orientadas enquanto que as LANs comuns implementam transmissão de dados sem conexão.

A utilização de LANE cria uma camada de conversão que mascara a conexão ATM para as aplicações que requerem transferência de dados sem conexão realmente tenham este aspecto. LANE suporta, também, a transmissão de quadros (Frames) Ethernet e Token Ring sobre redes ATM de modo que a princípio não se façam necessárias modificações nas redes

já existentes. LANE utiliza redes ATM como Backbones para interligar as diferentes tecnologias de redes LAN existentes.

Em resumo, o LANE define uma interface de serviço para os protocolos da camada de Data Link (nível 2) que é idêntico à existente camada MAC não implicando em alteração para os protocolos e aplicações das camadas superiores. Os dados enviados pela rede ATM são encapsulados em pacotes LAN MAC. A LANE funciona como uma ponte (transparente) que transporta o tráfego entre as suas duas LANs.

Vantagens E Desvantagens Do ATM

A tecnologia ATM oferece vários benefícios, quando comparada com outras tecnologias:

- Emprega a multiplexação estatística, que melhora muito o uso de banda;
- Faz o gerenciamento dinâmico de banda;
- O custo de processamento das suas células de tamanho fixo é baixo;
- Integra vários tipos diferentes de tráfego (dados, voz e vídeo);
- Garante a alocação de banda e recursos para cada serviço;
- Possui alta disponibilidade para os serviços;
- Suporta múltiplas classes de Qualidade de Serviço (QoS);
- Atende a aplicações sensíveis ou não a atraso e perda de pacotes;
- Aplica-se indistintamente a redes públicas e privadas;
- Pode compor redes escaláveis assim como flexíveis e com procedimentos de recuperação automática de falhas;
- Pode interoperar com outros protocolos e aplicações, tais como Frame Relay, TCP/IP, DSL, Gigabit Ethernet, tecnologia Wireless, SDH/SONET, entre outros.

Entretanto, sua utilização irrestrita tem encontrado alguns obstáculos, tais como:

- Outras tecnologias, tais como FastEthernet, GigabitEthernet e sobre elas o TCP/IP, têm sido adotadas com grande frequência em redes de dados;
- O uso de interfaces ATM diretamente aplicadas em PCs, estações de trabalho e servidores de alto desempenho não tem sido tão grande como se esperava a princípio.

Conclusões

Portanto, a tecnologia ATM introduziu conceitos novos e diferentes daqueles comumente utilizados em redes locais de computadores e quando uma rede ATM local é projetada, vários tipos de conexões são previstos entre um ou mais subsistemas.

Os subsistemas são conexões que envolvem normalmente a rede local e outras redes públicas (prestadores de serviços de telecomunicações) e que necessitam da definição de uma interface de serviço para os protocolos da camada de rede idêntico a existente na camada MAC, não implicando em alteração para os protocolos e aplicações das camadas superiores.

Outro ponto importante está em que um LANE não é capaz de emular todas as características da camada física e camada de enlace, mas deve possibilitar a interconexão de LANs tradicionais com LANs emuladas, mantendo o endereço MAC (Media Access Control) de cada dispositivo da LAN para, deste modo, preservar a base de aplicações existentes, permitindo que funcionem sem alterações sobre uma rede ATM.

UNIDADE 23

Objetivo: Entender e compreender a importância da tecnologia de Voz sobre IP (VoIP).

Tecnologias de Redes (Parte II)

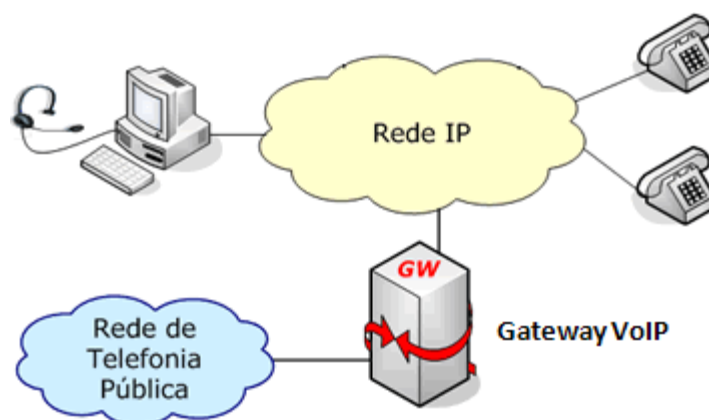
Voz over IP (VoIP)

O suporte às comunicações de voz utilizando o protocolo Internet (IP), mais comumente chamado de VoIP, ou "Voz sobre IP", torna-se um atrativo, principalmente, pelo baixo custo. De fato, a busca por uma boa qualidade de telefonia em redes IP é um dos passos-chave em direção à convergência das indústrias de voz, vídeo e comunicação de dados. VoIP pode ser definida como a habilidade de se fazer chamadas telefônicas (por exemplo, operar todas as facilidades oferecidas hoje pela rede de telefonia convencional) e enviar FAX em redes de dados baseadas em IP com um padrão de qualidade de serviço (QoS) aceitável e um custo/benefício superiores.

A primeira medida de sucesso dos Gateways VoIP é a redução de custos das ligações de longa distância sem adicionar inconvenientes ao usuário final, como, por exemplo, a necessidade de usar um microfone em um PC, ou mesmo configurações complicadas para se realizar uma chamada. Os Gateways VoIP possibilitam transportar chamadas telefônicas através das redes de dados em tempo real, sem atrasos e com excelente claridade de voz.

Estes equipamentos foram desenvolvidos dentro do conceito de otimização da empresas, caracterizados pela convergência de serviços de voz e dados e utilização de tecnologias de padrão aberto. O Gateway de VoIP com 2 interfaces FXS que permitem sua ligação direta em troncos analógicos de PABX (Private Automatic Branch Exchange) ou mesmo

diretamente em aparelhos telefônicos. A funcionalidade do Gateway VoIP provê serviços de Voz sobre IP (VoIP) com uma excelente relação custo/benefício para interligação de escritórios. Caso a empresa possua PABX coorporativo, o Gateway VoIP deve ser conectado aos troncos analógicos. Caso não possua PABX, o Gateway VoIP deve ser conectado a aparelhos telefônicos.

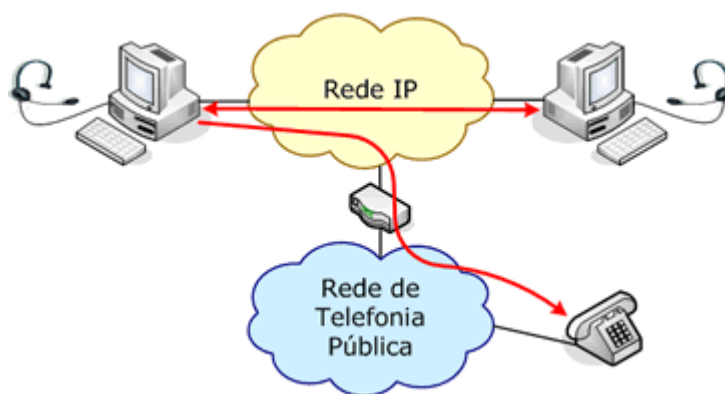
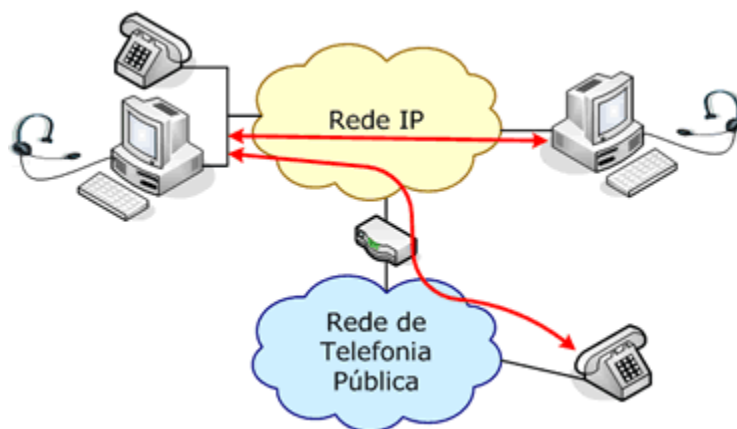
Em ambos os casos, o Gateway VoIP permite comunicação entre os ramais dos escritórios. As formas de utilização do Gateway VoIP podem ser do tipo Ponto-a-Ponto ou através de um gerenciador fazendo um roteamento IP do equipamento. O Gateway VoIP assegura uma alta performance e uma qualidade de voz bastante boa. É possível trabalhar com vários padrões de compressão de voz, além de mecanismos utilizados para assegurar maiores níveis de claridade de voz com menor utilização de banda.

Para uma empresa ter uma solução VoIP é necessário realizar um estudo da empresa através do qual sejam obtidas todas (ou quase todas) as necessidades que a empresa precisaria para, dessa maneira, saber (de forma clara) qual a solução que esta pode chegar a ter.

Algumas questões básicas podem ser respondidas, por exemplo, saber se a empresa possui Internet com IP fixo ou IP Dinâmico? Qual o tamanho da capacidade de transferência do canal ADSL da empresa? Qual o volume de dados (tráfego) que normalmente a empresa gera diariamente na Internet? Etc. Para que VoIP tenha uma boa funcionalidade entre ligações ponto-a-ponto é necessário ter um canal ADSL nas duas pontas.

Uma das principais vantagens da implantação de uma solução de VoIP em uma rede corporativa é a possível diminuição de custos com ligações telefônicas locais, interurbanas e até mesmo internacionais. Como as conversações telefônicas possuem as características de tráfego em tempo-real onde os atrasos no envio dos pacotes VoIP devem ser minimizados para não degradar muito o serviço, faz-se necessário utilizar uma série de subsídios extras para garantir a qualidade do serviço das ligações. Nesse sentido a tecnologia VoIP pode ser uma alternativa bastante viável e confiável para empresas que necessitam reduzir seus custos com ligações de longa distância.

Telefonia IP

Telefonia IP é a aplicação direta de VoIP para estabelecer chamadas telefônicas com a rede de telefonia pública (fixa e celular). Os serviços de Telefonia IP existentes são de 2 tipos:

1. **Para fazer chamadas para rede pública**: Neste caso o usuário disca o número convencional do telefone de destino para completar a chamada.

2. **Para fazer e receber chamadas da rede pública**: Aqui o usuário recebe um número convencional de telefone, para receber as chamadas da rede pública, e disca o número convencional do telefone de destino para fazer a chamada para a rede pública.

Em ambos os casos, o usuário pode fazer e receber chamadas de outro usuário do mesmo prestador de serviços VoIP, geralmente sem custo, porém não consegue chamar usuários de outros provedores VoIP.

As Interfaces FXS e FXO

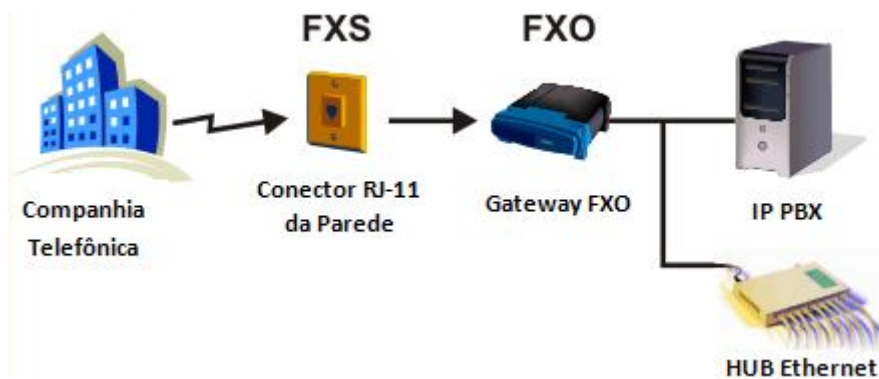
A interface FXS (Foreign eXchange Subscriber) fornece a linha analógica ao assinante. Em outras palavras, é o "conector na parede" que fornece o tom de discagem, e os níveis de voltagem e corrente para uma correta operação com a rede pública de telefonia.

A interface FXO (Foreign eXchange Office) recebe a linha analógica. É o conector no telefone ou aparelho de Fax, ou o(s) conectore(s) no seu sistema de telefonia analógica. Esta interface indica se o telefone está no gancho ou fora do gancho (circuito fechado). Como a interface FXO está ligada a um dispositivo, tal como o Fax ou telefone, esse dispositivo é normalmente chamado de "dispositivo FXO".

Portanto, FXS e FXO são as interfaces utilizadas pelas linhas de telefonia analógica, estas linhas analógicas são também conhecidas como POTS (Plain Old Telephone Service), ou seja, são as linhas analógicas do serviço telefônico tradicional. As interfaces FXO e FXS estão sempre em pares, de modo semelhante a um conector macho/fêmea. Caso não se faça uso de um PBX (Private Branch Exchange), um telefone fica conectado diretamente à porta FXS fornecida pela companhia telefônica, como ilustrado na figura.

No caso de ter um PBX (figura abaixo), as linhas fornecidas pela companhia telefônica estarão conectadas ao PBX, assim como os telefones. Portanto, o PBX deve ter tanto as portas FXO (para conectar com as portas FXS fornecidas pela companhia telefônica) assim como as portas FXS (para conectar os aparelhos de telefone e fax).

O Gateway FXO

Para conectar linhas telefônicas analógicas a um IP-PBX, você precisa de um Gateway FXO. Este dispositivo permitirá conectar a porta FXS à porta do Gateway, o que transforma uma linha telefônica analógica em uma linha disponível para realizar uma ligação VoIP.

O Gateway FXS

O Gateway FXS é usado para conectar uma ou mais linhas de um PBX convencional a um sistema de telefonia VoIP ou a um provedor. É preciso um gateway FXS para conectar as portas FXO (que normalmente estão conectadas à companhia telefônica) à Internet ou a um sistema VoIP.

Adaptador FXS (Adaptador ATA)

O adaptador FXS é usado para conectar o telefone ou fax analógico a um sistema de telefonia VoIP ou a um provedor VoIP. É necessário porque é preciso conectar a porta FXO do telefone (ou aparelho de fax) ao adaptador.

Como Escolher Entre Interfaces FXS e FXO?

Depende muito da aplicação e do tipo de central PABX que se disponha em lugares distintos da rede. Interfaces FXS são como linhas principais, ou seja, facilmente tomadas por qualquer

ramal para tráfego de saída, porém elas possuem o inconveniente de precisar ser "atendida" quando chega uma ligação. Interfaces FXO, ao contrário, são muito boas para tráfego de entrada, já que se comportam como ramal, ou seja, podem fazer tudo o que um ramal faz, sendo mais independente dos recursos do PABX. Para tráfego de saída, porém é necessário antes discar para um ramal para ser atendido pelo Gateway, antes de qualquer operação.

Procedimentos FXS/ FXO

A seguir se dão brevemente os detalhes técnicos sobre o funcionamento (ou procedimento) das interfaces FXS/ FXO para as seguintes tarefas:

- Realizar uma chamada externa:
    1. Retirar o telefone (dispositivo FXO) do gancho. A porta FXS detecta que o telefone está fora do gancho e passa o sinal de linha livre para o usuário.
    2. Digitar o número de telefone externo, este número será transmitido à porta FXS pelo uso comum de tom duplo multifrequência também conhecido como DTMF (Dual Tone Multifrequency). Este mecanismo DTMF é o padrão de todos os telefones atuais.
- Realizar uma chamada interna:
    1. A porta FXS recebe a ligação, e então envia um tom ao dispositivo FXO conectado.
    2. O telefone toca.
    3. Assim que alguém atende, a comunicação entre os usuários internos da corporação é iniciada.
- Finalizar uma chamada: Normalmente a porta FXS conta com qualquer dispositivo FXO conectado para finalizar a ligação.

Nota: A linha de telefonia analógica transmite aproximadamente um sinal de 50 volts de corrente continua (DC) à porta FXS. Devido a isso é que algumas pessoas poderiam sentir um “leve” choque ao tocar numa linha telefônica conectada.

Telefonia Convencional vs. VoIP

Característica	Telefonia Convencional	Telefonia VoIP
Conexão na casa do usuário	Cabo de cobre (par trançado)	Tecnologia ADSL banda larga com a Internet.
Falta de Energia Elétrica	Continua funcional	Para de funcionar.
Mobilidade	Limitada a casa do usuário	Acesso em qualquer lugar do mundo, desde que conectado à Internet.
Número Telefônico	Associado ao domicílio do usuário	Associado à área local do número contratado.
Chamadas locais	Área local do domicílio do usuário	Área local do número contratado.

Da mesma forma que na Internet, os serviços VoIP são Nômades, ou seja, não importa qual a localização física do prestador do serviço VoIP ou do usuário para que o serviço seja utilizado. O número telefônico, no entanto, não é nômade e está associado à área local do número contratado.

Dispositivos Utilizados Para VoIP

Os serviços VoIP utilizam aparelhos apropriados para as redes IP, e que são muito diferentes, em complexidade, começando pelos telefones analógicos convencionais devidamente adaptados (com conectores ATA), passando pelos computadores comuns até, propriamente, os telefones IP digitais que possuem recursos semelhantes aos encontrados nos computadores.

A seguir uma descrição destes dispositivos utilizados na tecnologia VoIP:

- **Computador**: O primeiro dispositivo utilizado como um terminal de telefonia IP foi o próprio computador. Este pode ser usado como telefone IP, desde que tenha uma placa de som instalada, microfone e alto falantes (ou fones de ouvidos), e um programa do tipo **Softphone** (por exemplo, o Skype) que possui todos os recursos para funcionar como um telefone IP.

- **Adaptador para Telefone Analógico**: Mais conhecidos como adaptadores ATA (Analog Telephone Adapter) é um dispositivo que funciona como um conversor de telefone IP para um telefone analógico convencional e vice-versa, ou seja, permite que um telefone comum possa se conectar através de uma rede VoIP.

O adaptador ATA é conectado diretamente a uma porta de acesso de banda larga ADSL e a um telefone analógico convencional, que pode ser usado normalmente para fazer e receber ligações através do serviço contratado de VoIP. Normalmente estes dispositivos vêm com um conector FastEthernet (RJ-45) e um conector para cabo telefônico RJ-11. Os adaptadores ATA são conhecidos também com os seguintes nomes: Gateways VoIP, adaptadores de terminal TA (Teminal Adapters), adaptadores FXS, etc. Alguns adaptadores ATA são configurados para trabalhar com um determinado provedor de serviços desta forma não sendo úteis para operar com outro provedor.

- **Telefone IP**: É um telefone que possui todos os recursos necessários para um serviço de telefonia utilizando a Internet para fazer e receber ligações via o serviço VoIP. Para fazer uso de um telefone IP é necessário apenas conectá-lo a um acesso de banda larga, por exemplo, desde uma rede LAN ou desde o domicilio através de uma linha ADSL, normalmente as configurações destes dispositivos não são complexas.

Basicamente o telefone IP converte e comprime o sinal de voz em pacotes de dados que serão enviados diretamente à Internet, em lugar de utilizar uma conexão da rede de telefonia pública normal.

Protocolos Da Tecnologia VoIP

Atualmente a grande maioria dos adaptadores ATA assim como os telefones IP fazem uso (de um) dos seguintes protocolos padrões da tecnologia VoIP:

1. **SIP (Session Initialization Protocol)**: É um protocolo de sinalização para telefonia IP utilizado para estabelecer, modificar e terminar ligações VoIP. SIP foi desenvolvido pelo IETF e publicado no documento RFC 3261. O SIP descreve os processos necessários para estabelecer uma ligação telefônica. Os detalhes deste procedimento estão descritos no protocolo SDP (Session Description Protocol) que descreve (na RFC 4566) os parâmetros de inicialização de uma sessão de mídia. Basicamente o protocolo SIP parece muito com o protocolo HTTP, utiliza um navegador como interfase com o usuário, este navegador é baseado em texto, relativamente de fácil manejo e muito flexível. O SIP tem amplamente substituído ao protocolo H.323, principalmente devido à enorme complexidade envolvida do protocolo H.323.

2. **IAX (Inter-Asterisk eXchange Protocol)**: É um protocolo de controle e transmissão de mídia (voz, vídeo) através de redes IP. Foi desenvolvido por Mark Spencer (criador do Asterisk, um servidor, do tipo central telefônica PBX de código aberto) e Frank Miller como uma alternativa aos protocolos já existentes, como o SIP e o H.323. Assim como o SIP, o IAX pode ser utilizado para qualquer tipo de sessão, seja de voz, vídeo, ambos ou outras. Apesar de poder ser usado para qualquer tipo de sessão, o IAX tem como foco principal o controle de chamadas usando VoIP. O IAX, também, tenta minimizar a quantidade de banda utilizada em uma transmissão e fornecer suporte nativo a NATs transparentes.

Vantagens Do Protocolo IAX Sobre O Protocolo SIP

Algumas vantagens do IAX sobre o SIP são apresentadas a seguir:

- É um protocolo bem mais simples se comparado ao SIP.
- Utiliza a mesma porta (4569/UDP) para administrar a sessão e fazer o transporte dos dados.
- No SIP, às vezes ocorre de uma chamada ter sido feita com sucesso porém o áudio não chega aos clientes. No IAX isso não ocorre, pois tanto o estabelecimento da sessão quanto o transporte dos dados são feitos pela mesma porta. Isso quer dizer que, se a porta usada pelo IAX não estiver bloqueada, os dados e o áudio serão transferidos com sucesso.

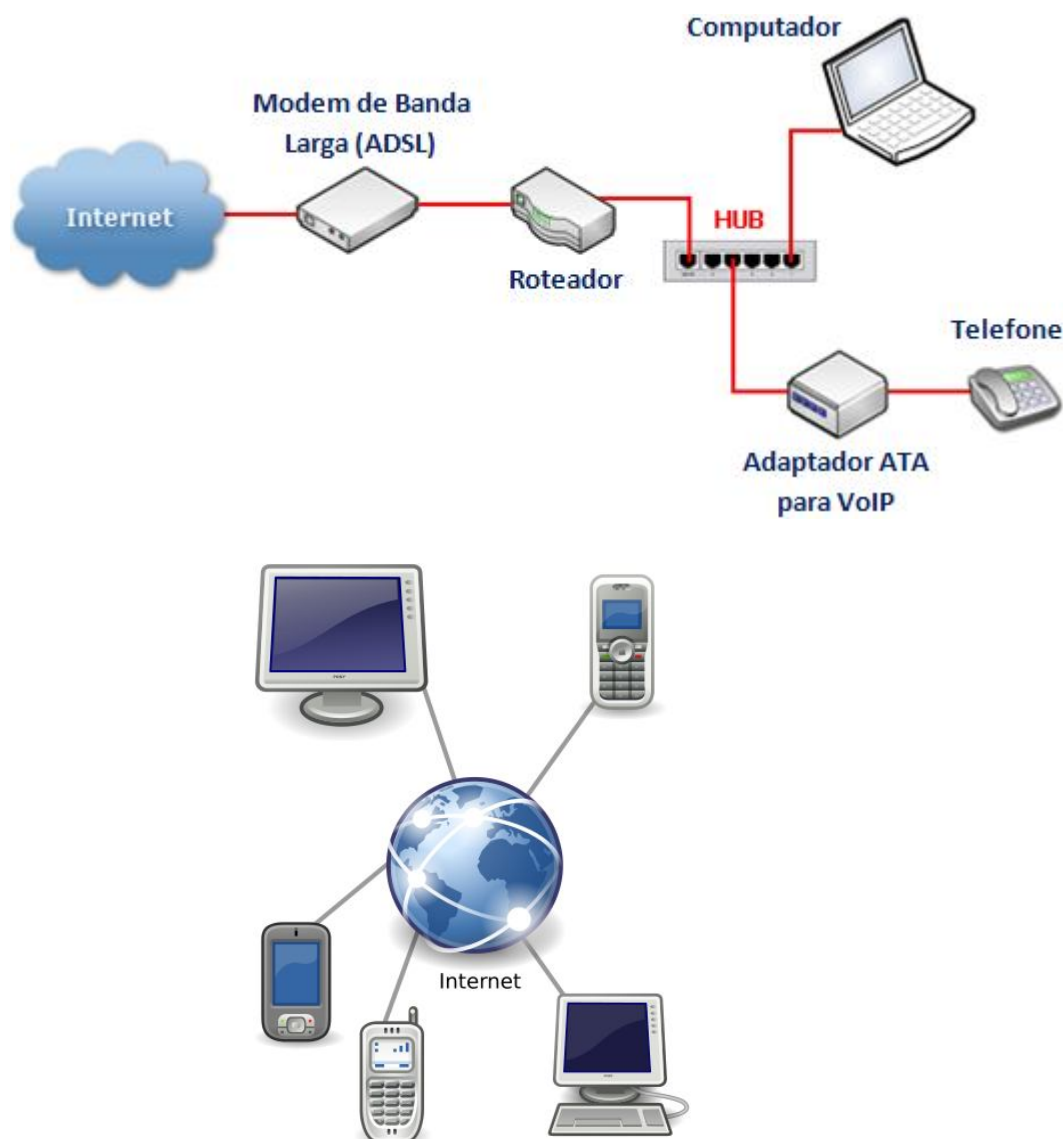
Regulamentação De VoIP

A Agencia Nacional de Telecomunicações (Anatel), assim como a maioria dos órgãos regulatórios no mundo, procura regular o serviço de telecomunicações e não as tecnologias usadas para implementá-los. As tecnologias VoIP servem como meio e não como fim para os serviços de telefonia. Não existe ainda uma regulamentação específica para VoIP no Brasil.

Entretanto, devido ao novo paradigma os serviços VoIP têm sido oferecidos no mercado de telecomunicações distribuídos em 4 classes:

- **Classe 1**: Oferta de um Programa de Computador que possibilite a comunicação de VoIP entre 2 (dois) ou mais computadores (PC a PC), sem necessidade de licença para prestação do serviço.
- **Classe 2**: Uso de comunicação VoIP em rede interna corporativa ou mesmo dentro da rede de um prestador de serviços de telecomunicações, desde que de forma transparente ao usuário. Neste caso, o prestador do serviço de VoIP deve ter pelo menos a licença SCM (Serviço de Comunicação Multimídia).

- **Classe 3**: Uso de comunicação VoIP irrestrita, com numeração fornecida pelo Órgão Regulador e interconexão com a Rede Pública de Telefonia (Fixa e Móvel). Neste caso o prestador do serviço de VoIP deve ter pelo menos a licença STFC (Serviço Telefônico Fixo Comutado).

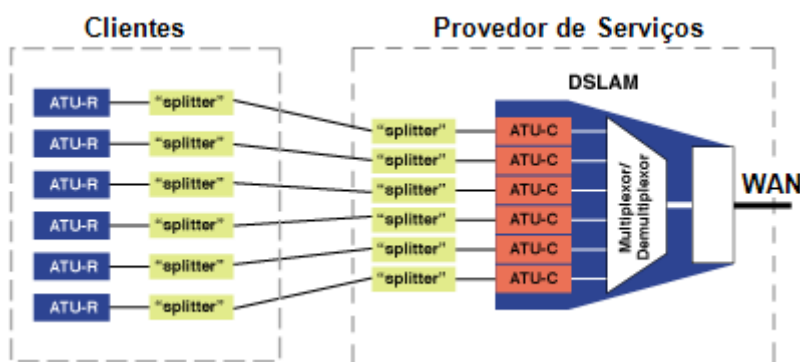
- **Classe 4**: Uso de VoIP somente para fazer chamadas, nacionais ou internacionais. Neste caso a necessidade de licença depende da forma como o serviço é caracterizado, e de onde (Brasil ou exterior) e por qual operadora é feita a interconexão com a rede de telefonia pública.

UNIDADE 24

Objetivo: Entender os princípios de funcionamento da tecnologia ADSL.

Tecnologias de Redes (Parte III)

ADSL

ADSL é a sigla para Assymmetric Digital Subscriber Line que traduzido seria algo assim como a "Linha Digital Assimétrica para o Assinante". Trata-se de uma tecnologia que permite a transferência digital de dados em alta velocidade por meio de linhas telefônicas comuns. A cada dia, a tecnologia ADSL ganha novos usuários, tanto é que gradualmente esta se transformando na tecnologia (em banda larga) de conexão à Internet mais utilizada no Brasil e uma das mais conhecidas no mundo.

A arquitetura fica completamente transparente com a inclusão da função do Splitter (divisor) e do DSLAM (Digital Subscriber Line Access Multiplexer) que é um conjunto de placas que possuem (cada uma) vários modems ATU-C (ADSL Terminal Unit-Central) e desta forma realiza a multiplexação de todas as conexões ADSL para uma rede WAN.

A comunicação do DSLAM para com o modem ADSL se realiza através de duas interfases denominadas ATU-R (ADSL Terminal Unit-Remote) que fica do lado do cliente e ATU-C (ADSL Terminal Unit-Central) a que esta do lado do provedor de serviços. Na frente de cada

um deles se coloca o Splitter. Basicamente, a função do Splitter é um filtro/misturador que, como o próprio nome indica, divide o espectro do sinal recebido em duas partes:

1. Uma parte, nas baixas frequências, para o sinal voz convencional, onde é possível fazer uso do serviço telefônico (fax) tradicional e
2. A outra parte, nas altas freqüências, para a transmissão (Upload) e recepção (Download) de dados entregues ao modem (ou roteador) ADSL.

É justamente devido às funções conjuntas do Splitter e do DSLAM que não existe interferência entre os dois serviços, daí a possibilidade da utilização da linha telefônica no modo convencional ao mesmo tempo em que se utiliza a Internet.

Funcionamento Da Tecnologia ADSL

A tecnologia ADSL basicamente divide a linha telefônica em três canais virtuais, sendo um para voz, um para **Download** (de velocidade alta) e um para **Upload** (com velocidade média se comparado ao canal de Download). Teoricamente, as velocidades de Download podem ir de 256 Kbps até 6.1 Mbps. No caso do Upload essas taxas variam de 16 Kbps até 640 Kbps, mas tudo dependerá da infraestrutura do fornecedor do serviço, o que indica que essas taxas podem ter valores diferentes dos mencionados. É por causa dessas características que o ADSL ganhou o termo "Assymmetric" (assimétrico) no nome, pois indica que a tecnologia possui maior velocidade para Download e menor velocidade para Upload.

Repare que nas baixas freqüências se encontra o canal de voz para o serviço telefônico convencional. Isso permite que o usuário fale ao telefone e ao mesmo tempo navegue na Internet, ou seja, não é necessário desconectar a Internet para falar ao telefone. Como explicado anteriormente, para separar o canal de voz do canal de dados é instalado (na linha telefônica do usuário) um pequeno aparelho chamado Splitter. Nele é conectado um cabo que sai do aparelho telefônico e outro que sai do modem.

Na central telefônica também existe um Splitter. Assim, quando você realiza uma chamada telefônica (voz), o sinal é encaminhado para a rede de comutação de circuitos da companhia telefônica PSTN (Public Switched Telephone Network) e procede pelo seu caminho habitual. Quando você utiliza a Internet, o sinal é encaminhado ao DSLAM, que é explicado logo abaixo.

Quando uma linha telefônica é usada somente para voz, as chamadas utilizam frequências baixas, geralmente entre 300 Hz e 4 kHz. Na linha telefônica é possível usar taxas mais altas, mas elas acabam sendo desperdiçadas. Explicando de maneira simples, o que o ADSL faz é aproveitar para a transmissão de dados as frequências que não são utilizadas. Como é possível utilizar mais de uma frequência ao mesmo tempo na linha telefônica, é então possível usar o telefone para voz e dados ao mesmo tempo. A ilustração abaixo exemplifica este esquema.

Voz	Upload	Download

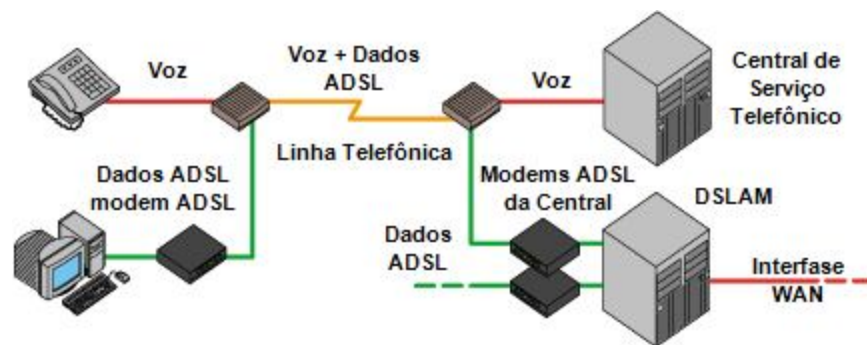
300 Hz 4 kHz 2.2 MHz

A tecnologia ADSL funciona instalando-se um modem específico para esse tipo de conexão na residência ou empresa do usuário e fazendo-o se conectar a um equipamento na central telefônica. Neste caso, a linha telefônica serve como "estrada" para a comunicação entre esses dois pontos. Essa comunicação ocorre em frequências acima de 5 kHz, não interferindo na comunicação de voz (que funciona entre 300 Hz e 4 kHz).

Como a linha telefônica é usada unicamente como um meio de comunicação entre o modem do usuário e a central telefônica, não é necessário pagar pulsos telefônicos, pois a conexão ocorre por intermédio do modem e não discando para um número específico, como é feito com o acesso à Internet via conexão discada. Isso deixa claro que todo o funcionamento do ADSL não se refere à linha telefônica, pois esta é apenas um "caminho", mas sim ao modem.

Quando seu modem estabelece uma conexão com o modem da central telefônica, o sinal vai para um roteador, em seguida para o provedor e finalmente para a Internet. É importante

frisar que é possível que este sinal saia diretamente do roteador para a Internet. No Brasil, o uso de provedor é obrigatório por regras da Anatel (Agência Nacional de Telecomunicações). No entanto, essa questão não será discutida aqui.

O sinal citado acima, depois de enviado à central telefônica, é separado e os dados vão para um equipamento DSLAM (Digital Subscriber Line Access Multiplexer), que limita a velocidade do usuário e une várias linhas ADSL, é este equipamento que permite a você navegar a 256 Kbps mesmo quando sua conexão suporte 2 Mbps. Após disso o sinal é enviado para uma interfase WAN (por exemplo, uma linha ATM) que conecta à Internet. Em outras palavras, a central telefônica suporta certa quantidade de usuários ao mesmo tempo. Cabe ao DSLAM gerenciar todas essas conexões, "agrupá-las" e enviar esse grupo de conexões ao canal ATM, como se fosse uma única conexão.

Praticamente todas as empresas que fornecem ADSL só o fazem se o local do usuário não estiver a mais de 5 Km da central telefônica. Quanto mais longe estiver, menos velocidade o usuário pode ter e a conexão pode sofrer instabilidades ocasionais. Isso se deve ao ruído (interferência) que ocorre entre um ponto e outro. Quanto maior essa distância, maior é a taxa de ruído. Para que haja uma conexão aceitável é utilizado o limite de 5 Km. Acima disso pode ser possível, mas inviável o uso de ADSL.

O emprego de modem ou de um router depende da utilização que se pretende dar à conexão. Se o uso será apenas com um PC, então a opção adequada é um modem; se a conexão será compartilhada numa rede de computadores o router é o equipamento indicado. É tecnicamente possível, contudo, compartilhar a conexão quando se utiliza um modem, mas

nesta situação é necessário um equipamento que sirva de interface entre o modem ADSL e a rede local (Hub/Proxy Server).

Quanto à qualidade, esta pode ser prejudicada por vários fatores, dentre eles a distância entre o terminal telefônico da central. Esse problema é mais notável nas regiões interioranas, onde existem duas ou três centrais para atender a todo o município. Outro problema comum pode estar na fiação interna da casa do usuário, como também no cabeamento externo da rede, que sofrem deterioração com a ação do tempo comprometendo a comunicação entre os modems causando instabilidade na conexão.

Uma grande vantagem da banda larga ADSL é o uso da linha telefônica como meio de comunicação entre o modem do usuário e o da central, sem a contagem e tarifa por pulsos. Entretanto tal vantagem pode estar com os dias contados, ou pelo menos tende a ser minimizada pelas cotas de volume de tráfego que os provedores vêm determinando. Sendo assim, cada plano oferecerá um limite, que se ultrapassado, será cobrado separadamente.

Basicamente os diferentes dispositivos utilizados em uma conexão ADSL (conforme a figura acima) através de um provedor de serviços ISP (que utiliza uma infra-estrutura ATM) são:

1. **O modem ADSL (do usuário):** É um elemento periférico que transforma a informação digital em analógica para poder transmiti-la pela linha telefônica. Faz a operação inversa quando recebe a informação.

2. **O filtro separador (Splitter):** O filtro separa a informação digital da analógica do lado do usuário.

3. **O cabo de cobre:** A tecnologia ADSL utiliza o cabo de cobre existente na linha telefônica. A voz e os dados são transmitidos de maneira simultânea, basta instalar pequenos equipamentos em cada extremo da linha.

4. **O marco de distribuição:** É uma conexão operadora que distribui a informação, neste ponto se encontram o Splitter e o DSLAM do provedor de serviços ISP.

5. **O servidor de acesso à banda larga BAS (Broadband Access Server):** Após o DSLAM, a informação compilada é centralizada e enviada ao BAS, este servidor dedicado é o encarregado de retransmitir para a Internet. Normalmente o servidor BAS é utilizado quando o provedor de serviços à Internet faz uso de uma infra-estrutura de rede ATM.

O Protocolo PPPoE

O ADSL por si só é um meio físico de conexão, que trabalha com os sinais elétricos que serão enviados e recebidos. Funcionando dessa forma, é necessário um protocolo para encapsular os dados de seu computador até a central telefônica. O protocolo mais utilizado para essa finalidade é justamente o PPPoE.

O PPPoE (Point-to-Point Protocol over Ethernet), ou seja, o protocolo Ponto-a-Ponto sobre Ethernet (documentado na RFC 2516), é um protocolo para conexão de usuários em uma rede Ethernet a Internet. Seu uso é típico nas conexões de um ou múltiplos usuários em uma rede LAN conectada à Internet através de uma linha DSL, de um dispositivo Wireless (sem-fio) ou de um modem de cabo Broadband comum. O protocolo PPPoE deriva do protocolo

PPP. O PPPoE estabelece a sessão e realiza a autenticação com o provedor de acesso a Internet.

Diante das informações acima, você deve se perguntar por que em muitos casos é necessário usar um programa para se conectar a Internet, se o ADSL permite uma conexão permanente usando unicamente o modem.

O protocolo PPPoE trabalha com a tecnologia Ethernet, que é usada para ligar sua placa de rede ao modem, permitindo a autenticação para a conexão e aquisição de um endereço IP à máquina do usuário. É por isso que cada vez mais as empresas que oferecem ADSL usam programas ou o navegador de Internet do usuário para que este se autentique. Autenticando, é mais fácil identificar o usuário conectado e controlar suas ações.

Você pode estar se perguntando: por que os primeiros serviços de ADSL do país davam IP fixo ao usuário, sem necessidade de usar o PPPoE, ou seja, porque o PPPoE não foi usado antes? Naquela época, o protocolo PPPoE era novo (foi homologado em 1999) e, consequentemente, pouco conhecido. Com isso, o usuário usava ADSL através de uma conexão direta do modem à central telefônica, sem necessidade de autenticar. Mas quando as empresas começaram a descobrir as vantagens do PPPoE passaram a implantá-lo. Isso permite que a companhia tenha mais controle sobre as ações do usuário.

Em resumo, O servidor PPPoE fica escutando por requisições de autenticação. Após o cliente ser autenticado com sucesso através de algum dos seguintes servidores RADIUS (Remote Authentication Dial In User Service) ou TACACS+ (Terminal Access Controller Access-Control System+), é criado um túnel entre o cliente e o servidor.

Supondo que se tenha um servidor RADIUS configurado com a faixa de endereços IPs que serão utilizados, o servidor atribuirá um endereço IP desta faixa para os clientes que tenham feito um login com sucesso. Esses IPs válidos podem ser fixos ou dinâmicos, dependerá só da necessidade.

UNIDADE 25

Objetivo: O porquê dos conceitos de segurança serem necessários.

Segurança em Redes (Parte I)

A segurança no universo computacional se divide em segurança lógica e segurança física, presentes tanto em computadores do tipo Stand-alone (monousuário) como em computadores ligados em rede (Internet ou Rede interna).

Segurança Física

Devemos atentar para ameaças sempre presentes, mas nem sempre lembradas: incêndios, desabamentos, relâmpagos, alagamentos, problemas na rede elétrica, acesso indevido de pessoas ao Centro de Processamento de Dados (CPD), treinamento inadequado de funcionários, etc.

Medidas de proteção física, tais como: serviços de guarda, assim como o uso de dispositivos No-breaks, alarmes, fechaduras, circuito interno de televisão e sistemas de escuta, são realmente uma parte da segurança de dados. As medidas de proteção física são frequentemente citadas como "segurança computacional", visto que têm um importante papel também na prevenção dos itens citados no parágrafo acima. O ponto-chave é que as técnicas de proteção de dados por mais sofisticadas que sejam não têm serventia alguma se a segurança física não for garantida.

Segurança Lógica

Esta requer um estudo maior, pois envolve investimento em softwares de segurança ou sua respectiva elaboração. Deve-se estar atento aos problemas causados por vírus, acesso de invasores de rede, programas de backup desatualizados ou feitos de maneira inadequada, distribuição de senhas de acesso, etc.

Um recurso muito utilizado para proteger-se dos invasores da Internet é a utilização de um programa de criptografia que embaralha o conteúdo da mensagem, de modo que ela se torne incompreensível para aqueles que não sejam seus receptores ou provedores.

O objetivo da segurança de redes abrange desde uma fechadura na porta da sala de computadores até o uso de técnicas criptográficas sofisticadas e códigos de autorização. Seu estudo não abrange somente o crime computacional (Crackers), mas também envolve qualquer tipo de violação da segurança, como erros em processamento ou códigos de programação no uso de informações (softwares e dados armazenados) no computador e os dispositivos de armazenamento associados a indivíduos selecionados.

Preservação do patrimônio da empresa: os dados e as informações fazem parte do patrimônio. Portanto, devem ser preservados protegendo-os contra revelações acidentais, erros operacionais (montagem errada de um disco magnético, por exemplo) e contra as infiltrações que podem ser de dois tipos:

- **Infiltração deliberada**: Os objetivos principais deste tipo de infiltração é a de poder acessar informações de arquivos importantes da empresa, descobrir os interesses da informação dos usuários, alterar ou destruir arquivos e obter livre uso dos recursos do sistema.

- **Infiltração ativa**: Envolve desde o exame periódico dos conteúdos das cestas de lixo da área do computador até a gravação clandestina dos dados armazenados. A infiltração ativa inclui:

- **Sapear**: É o uso do acesso legítimo ao sistema para obtenção de informação não autorizada;
- **Usar disfarce**: É a prática da obtenção de identificação própria por meios impróprios (como a gravação clandestina) e, a seguir, o acesso ao sistema como um legítimo usuário;
- **Detectar e usar alçapões**: São dispositivos de hardware, limitações de software ou pontos de entrada especialmente plantados que permitem que fonte não autorizada tenha acesso ao sistema;
- **Infiltração**: Fazendo uso de canais ativos de comunicações;

Os meios físicos incluem o acesso ao sistema por meio de uma posição no centro de computação, ou seja, profissionais que ocupam cargos com acesso ao CPD e deliberam as informações a terceiros; e o roubo de veículos removíveis de armazenamento.

- Manutenção dos serviços prestados pela empresa;
- Segurança do corpo funcional;
- Em caso de problemas: detecção das causas e origens dos problemas no menor prazo possível, minimização de suas consequências, retorno às condições normais no menor prazo, com a diminuição de custo e o menos traumática possível.
- Detecção e análise dos pontos vulneráveis;
- Estabelecimento de políticas de segurança (técnicas de segurança incluem aspectos do hardware computacional, rotinas programadas e procedimentos manuais, bem como os meios físicos usuais de segurança local e segurança de pessoal, fechaduras, chaves e distintivos);
- Execução das políticas de segurança;

- Acompanhamento;
- Avaliação dos resultados contra os objetivos traçados;
- Correção de objetivos e políticas;
- Gerência de acesso, ou controle de acesso, trata da prevenção para que usuários não autorizados obtenham serviços do sistema computacional ou tenham acesso aos arquivos. Esse controle é mais complicado quando se trata de rede, já que qualquer um pode se passar por usuário autorizado, daí a importância do uso de técnicas de segurança, como senhas ou identificação por cartões magnéticos;

Esse controle deve considerar os seguintes fatores:

- **Conteúdo das informações**: Refere-se à sensibilidade dos programas e dados que possam exigir uma das seguintes coisas: nenhuma providência sobre segurança de dados, restrições normais a necessidades de conhecimento, ou preocupações extensas para evitar revelação.
- **Ambiente**: Refere-se aos usuários e aos métodos pelos quais eles têm acesso ao sistema.
- **Comunicações**: Referem-se ao uso da facilidade das comunicações de dados, no local do computador, por meio de uma rede privada ou pode ser uma rede pública.
- **Facilidades de sistema**: Referem-se a serviços previstos pelo sistema computacional que podem incluir, no mínimo, funções especializadas, solução de problema interativo, apoio remoto de programação e um sistema total de informação.

Basicamente, deve ser criado um Plano de Segurança (como evitar problemas) e um Plano de Contingência (o que fazer em caso de problemas). É importante frisar que segurança absoluta não existe. Trata-se de descobrir os pontos vulneráveis, avaliar os riscos, tomar as

providências adequadas e investir o necessário para ter uma segurança homogênea e suficiente. Sempre existirão riscos, o que não se pode admitir é o descaso com a segurança.

Os princípios básicos da segurança são:

- Autenticidade,
- Confidencialidade,
- Integridade e
- Disponibilidade das informações.

Os benefícios evidentes são: reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas, para aumentar a produtividade dos usuários por meio de um ambiente mais organizado, maior controle sobre os recursos de informática e, assim, viabilizar aplicações críticas das empresas.

Quando se utiliza a Internet, rastros ocultos e expressos são deixados em diversas formas e em diversas partes do sistema. É possível (através da coleta dessas informações em um dado período de tempo) utilizar análise estatística e comparação, para traçar os interesses pessoais de um usuário (suas preferências de conteúdo acessado na Internet, quais as páginas e que tipo de páginas recebem sua maior atenção), conteúdo de correios eletrônicos, imagens, áudio entre outras coisas mais. Essa informação também pode ser utilizada para detectar se existiu (ou existe) algum tipo de infiltração externa ao sistema por parte de pessoas alheias à corporação.

Algumas Possibilidades De Ameaças

- **Hackers e Crackers**: Hackers são em geral jovens e adolescentes, amadores aficionados por informática, normalmente com alto grau de inteligência e capacitação no ramo, cuja principal diversão é conseguir ultrapassar as barreiras de acesso aos

grandes sistemas de computação que operam em rede principalmente na Internet. Em geral, a atuação dos hackers não tem como finalidade a obtenção de vantagens econômicas para si; entretanto, são inúmeros os casos de violação de sistemas por parte de hackers que causam prejuízos sérios às organizações e, em diversos casos, colocaram em risco vidas humanas ao acessarem sistemas de hospitais. Os crackers além de espionar destroem e alteram as informações que encontram.

- **Vírus**: São programas projetados para serem copiados dentro de outros programas e pode causar perda ou alteração dos dados armazenados no computador. Em casos extremos pode destruir completamente dados armazenados, de forma a tornar o equipamento não operacional. O vírus é ativado quando o programa por ele "infectado" é executado.

- **Bomba Lógica**: É talvez a forma de modificação não autorizada em sistemas que é difícil de ser detectada e mais perigosa. É também conhecida como bomba relógio, pois na maioria dos casos o disparo é efetuado pela data do sistema, mas existem casos relacionados com os dados de entrada. O principal fator envolvido é um funcionário com um grande grau de conhecimento de informática e que, por um motivo qualquer, esteja descontente com a empresa.

- **Cavalo de Tróia**: O nome é relacionado ao fato de funcionar baseado em estratégia similar. O meio de infiltração geralmente está relacionado com o acesso e a forma assumida em geral é um jogo interessante e desafiador. Para poder jogá-lo, o usuário precisa iniciar uma sessão usando sua chave de acesso ao monitor e carregando o programa do jogo, que normalmente reside em uma biblioteca de uso público. Enquanto ele está se divertindo com o jogo, o programa pode estar apagando arquivos, alterando dados ou até copiando dados para um arquivo do hacker que fez o programa.

- **Alçapão**: Modo de acesso ao sistema que de outra forma não seria permitido; seu funcionamento é similar às passagens secretas dos castelos medievais. Normalmente permanecem escondidos e somente são usados quando necessários. Os Alçapões

são bastante comuns em ambientes de computadores de grande porte e quase sempre são obras dos próprios profissionais internos que, dessa forma, querem manter uma via de acesso que contorne a segurança.

Técnicas De Defesa

As técnicas estão relacionadas aos vários aplicativos que cuidam de aspectos diversos do problema e que podem ser usados para essa finalidade, como, por exemplo:

- Softwares de Administração de Redes;
- Softwares de Segurança;
- Softwares de Controle de Oficialização de novos programas;
- Aplicativos de Administração de espaço em disco;
- Análise do Sistema Operacional.

Entretanto nenhum dos pacotes acima é especificamente direcionado para pesquisa e combate a vírus. Esse tipo de tarefa deve ser feito mais no campo administrativo com medidas destinadas a disciplinar o uso de recursos, tais como:

- Chaves de acesso individuais (senhas) para cada funcionário autorizado a acessar facilidades computacionais, de modo que estabeleçam prontamente a cadeia de responsabilização;
- Gravação de programas executáveis nas bibliotecas de programas, efetuado somente através de meio de acesso mantido somente sob estrito controle;

- Registro permanente e fiscalização das atividades executadas em cima de tais tipos de bibliotecas;
- Documentação organizada;
- Evitar ao máximo o aumento de responsabilidades e funções nas mãos de poucas pessoas.

UNIDADE 26

Objetivo: O que é uma parede de fogo e como ela pode nos proteger.

Segurança em Redes (Parte II)

Firewall

Os Firewalls (paredes de fogo) são mecanismos muito utilizados para aumentar a segurança de redes conectadas à Internet. São uma espécie de barreira de proteção constituídas de um conjunto de hardware, software ou ambos que garantem uma política de controle de acesso entre duas redes (normalmente a Internet e uma rede LAN). Em princípio, os Firewalls podem ser vistos como um par de mecanismos: um que existe para bloquear o tráfego e outro para permitir o tráfego. Alguns Firewalls dão maior ênfase ao bloqueio de tráfego, enquanto outros enfatizam a permissão do tráfego, o importante é configurar o Firewall de acordo com a política de segurança da organização que o utiliza, estabelecendo o tipo de acesso que deve ser permitido ou negado.

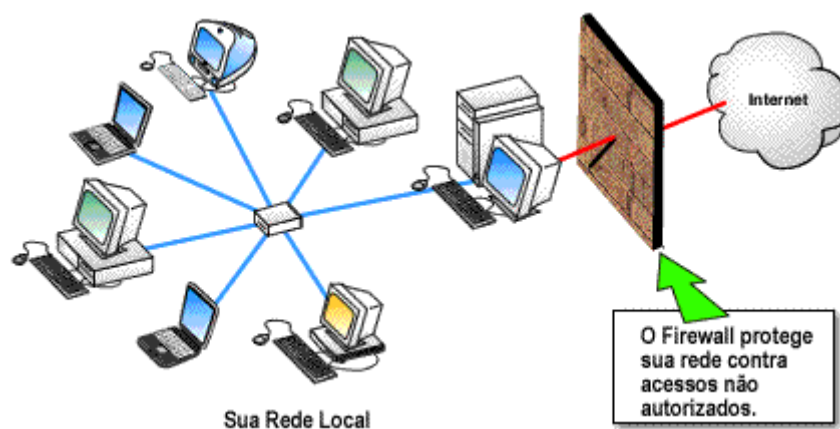
O Firewall é um quesito de segurança de muita importância no mundo da computação atual. À medida que o uso de informações e sistemas é cada vez maior, a proteção destes requer a aplicação de ferramentas e conceitos de segurança eficientes. O Firewall é uma opção praticamente imprescindível.

O conceito de Firewall é o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.

Este conceito inclui os equipamentos de filtros de pacotes e de Proxy de aplicações, comumente associados a redes TCP/IP. Tanto assim que os primeiros sistemas Firewall surgiram exclusivamente para dar segurança ao conjunto de protocolos TCP/IP.

Os Firewalls podem ser de três tipos:

1. Por software (programas ou aplicativos),
2. Por hardware (dispositivos físicos),
3. Ou pela combinação de ambos (neste caso, normalmente é chamado de "Appliance").

A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que autorizam o fluxo de entrada e saída de informações e do grau de segurança desejado.

Funcionamento De Um Firewall

Um Firewall é um dispositivo de segurança, veremos exatamente o que faz e em que baseia seu funcionamento. Como o próprio nome indica um Firewall é um dispositivo que funciona como corta-fogos entre redes, é uma “parede de fogo” geralmente entre uma LAN e a

Internet, permitindo ou denegando o fluxo de dados, normalmente, entre uma rede privada e a rede pública.

Um uso típico é situá-lo entre uma rede LAN e a Internet, como dispositivo de segurança para evitar que os intrusos possam acessar a informação confidencial da rede LAN.

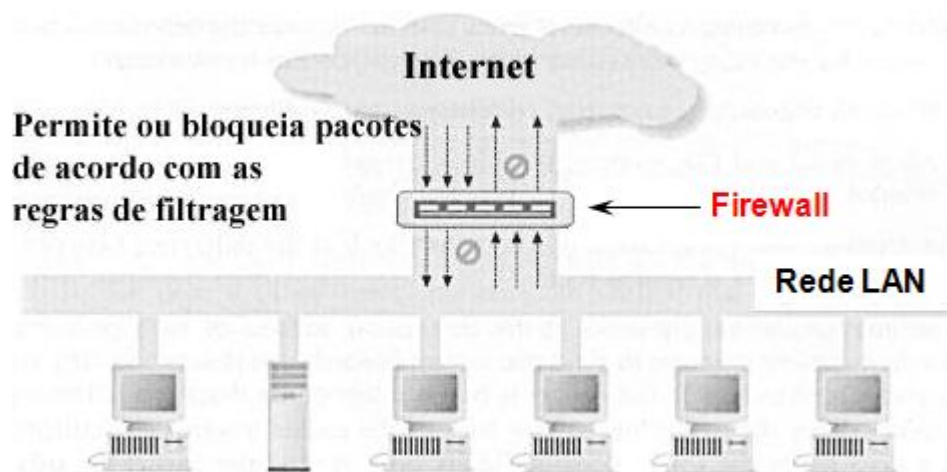
Basicamente o Firewall é um filtro que controla todas as comunicações que passam de uma rede a outra e em função do que sejam permite ou denega seu passo. Para permitir ou denegar uma comunicação o Firewall examina o tipo de serviço ao que corresponde, como podem ser a Web, o correio eletrônico ou os serviços IRC (Internet Relay Chat). Dependendo do serviço o Firewall decide se o permite ou não. Ademais, o Firewall examina se a comunicação está entrando ou saindo e dependendo da sua direção pode permiti-la ou não.

Deste modo, um Firewall pode permitir que uma rede LAN tenha acesso para a Internet, mas restringindo alguns serviços, isto é, o gerente da rede pode dar privilégios aos serviços de Web, tais como correio eletrônico, FTP, Telnet, SSh (Secure Shell) entre outros que são necessários para o nosso trabalho, mas poderia negar serviços tais como os serviços de IRC, Messenger MSN, ICQ, aplicativos P2P (Kazaa, Emule, etc.), que (na maioria dos casos) podem ser desnecessários para o nosso trabalho.

Também podemos configurar os acessos que se fazem desde a Internet para a rede local e podemos denegá-los todos ou permitir alguns serviços como o da Web, (se é que possuímos um servidor Web e queremos que seja acessível pela Internet). Dependendo do Firewall que tenhamos também poderemos permitir alguns acessos à rede local desde a Internet se o usuário tiver se autenticado como usuário da rede local.

Como mencionado anteriormente, um Firewall pode ser um dispositivo software ou hardware (ou uma mistura de ambos), ou seja, um pequeno aparelho conectado entre a rede e o cabo da conexão à Internet, ou então um programa que instalado na máquina que tem o modem que conecta com Internet. Inclusive podemos encontrar computadores muito potentes e com softwares específicos que simplesmente monitoram as comunicações entre redes.

Filtragem De Pacotes

O Firewall que trabalha na filtragem de pacotes é muito utilizado em redes LAN pequenas ou de porte médio. Por meio de um conjunto de regras estabelecidas, com este tipo de Firewall pode-se determinar que endereços IP podem transmitir/receber dados de sítios específicos da Internet. Alguns sistemas ou serviços podem ser liberados completamente (por exemplo, o serviço de e-mail), enquanto outros são bloqueados por padrão, por terem riscos elevados (como softwares de mensagens instantâneas, tais como o ICQ, MSN, mIRC, etc.) O grande problema deste tipo de Firewall, é que as regras aplicadas podem ser muito complexas e causar perda de desempenho da rede ou não serem o suficientemente eficazes.

Este tipo se restringe a trabalhar nas camadas de rede e transporte do TCP/IP, decidindo quais pacotes de dados podem passar e quais não. Tais escolhas são regras baseadas nas informações do endereço IP remoto, endereço IP do destinatário, além da porta TCP usada.

Quando devidamente configurado, esse tipo de Firewall permite que somente "computadores conhecidos troquem determinadas informações entre si e tenham acesso a determinados recursos". Um Firewall assim, também é capaz de analisar informações sobre a conexão e notar alterações suspeitas, além de ter a capacidade de analisar o conteúdo dos pacotes, o que permite um controle ainda maior do que pode ou não ser acessível.

Firewall De Aplicação

São Firewalls de controle de aplicação, por exemplo, as aplicações que utilizam dos protocolos SMTP (e-mail), FTP (transferência de arquivos), HTTP (transferência de hipertexto), etc. são geralmente instalados em servidores e são conhecidos como Proxy. Este tipo de dispositivo não permite comunicação direto entre a rede LAN e a Internet. Tudo deve passar pelo Firewall, que atua como um intermediador. O Proxy efetua a comunicação entre ambos os lados por meio da avaliação do número da sessão TCP dos pacotes.

Este tipo de Firewall é mais complexo, porém muito seguro, pois todas as aplicações precisam de um Proxy. Caso não haja, a aplicação simplesmente não funciona. Em casos assim, uma solução é criar um "Proxy genérico", através de uma configuração que informa que determinadas aplicações usarão certas portas. Essa tarefa só é bem realizada por administradores de rede ou profissionais de comunicação qualificados.

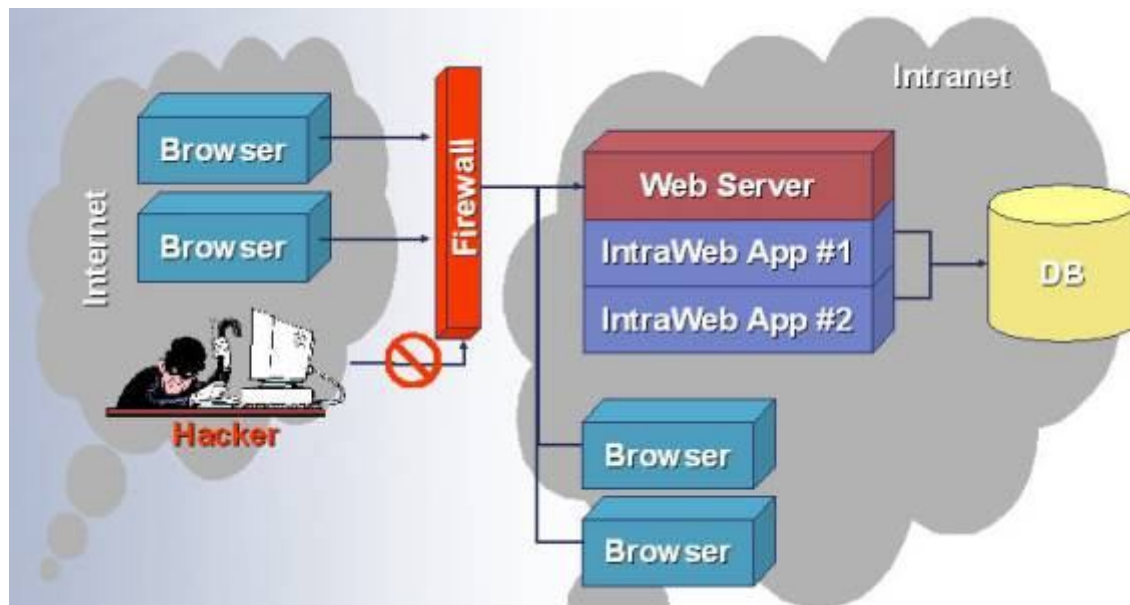
O Firewall de aplicação permite um acompanhamento mais preciso do tráfego entre a rede LAN e a Internet (ou entre redes LAN). É possível, inclusive, contar com recursos de login e ferramentas de auditoria. Tais características deixam claro que este tipo de Firewall é voltado a redes de porte médio ou grande e que sua configuração exige certa experiência no assunto.

Razões Para Utilizar Um Firewall

A seguir são citadas as 3 principais razões (segundo o InfoWester) para se fazer uso de um dispositivo de Firewall:

1. O Firewall pode ser usado para ajudar a impedir que sua rede ou seu computador seja acessado sem autorização. Assim, é possível evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers (ou o que seria pior de crackers);

2. O Firewall é um grande aliado no combate a vírus, cavalos de tróia, spywares e vermes, uma vez que é capaz de bloquear portas que eventualmente sejam utilizadas por essas "pragas digitais" ou então bloquear acesso a programas não autorizados;

3. Em redes corporativas, é possível evitar que os usuários acessem serviços ou sistemas indevidos, além de ter o controle sobre as ações realizadas na rede, sendo possível até mesmo descobrir qual usuário as efetuou.

Portanto, no quesito segurança física e lógica de uma rede LAN a importância de se ter um Firewall é obvia e cada vez maior, não somente para o uso em redes LAN corporativas, mas também para o uso doméstico. Nesse sentido, se você decide utilizar um Firewall em seu computador, procure por soluções conhecidas para seu sistema operacional (Windows, Linux, etc.). Existem soluções muito boas que são gratuitas (para uso doméstico), contam com configurações pré-definidas que exigem pouco conhecimento e não consomem muitos recursos do computador (assim como existem outras, que exigem experiência no assunto). Para administradores de rede, obviamente, o uso de um Firewall é tido como uma obrigação.

UNIDADE 27

Objetivo: Saber o conceito e funcionalidade de um servidor Proxy.

Segurança em Redes (Parte III)

Servidor Proxy

Um servidor Proxy[5] é um tipo de servidor que atua nas requisições dos seus clientes executando os pedidos de conexão a outros servidores. Um cliente conecta-se a um servidor Proxy, requisitando algum serviço tal como, servidor de arquivos, Web, ou outro recurso disponível em um servidor diferente.

O servidor Proxy disponibiliza este recurso solicitado a este cliente, conectando-se ao servidor que disponibiliza este recurso e o repassa ao cliente. Um servidor Proxy pode, opcionalmente, alterar a requisição do cliente ou a resposta do servidor e, algumas vezes, pode disponibilizar este recurso sem nem mesmo se conectar ao servidor especificado.

Um servidor Proxy pode ser disponibilizado no computador local do usuário ou em pontos estratégicos entre o usuário e o servidor de destino ou a Internet. Pode também atuar como um servidor que armazena dados em memória cache (que é a memória intermédia entre a memória RAM e os discos rígidos) em redes LAN. Os servidores Proxy são instalados em máquinas com conexões tipicamente superiores às dos clientes e com poder de

[5] A tradução da palavra inglesa Proxy, segundo o dicionário Michaelis, significa procurador, substituto ou representante.

armazenamento elevado. É de salientar que, utilizando um Proxy, o endereço que fica registrado no(s) servidor(es) é o do próprio Proxy e não o do cliente.

O Proxy surgiu da necessidade de conectar uma rede LAN à Internet através de um computador da rede que compartilha sua conexão com as demais máquinas. Em outras palavras, se considerarmos que a rede local é uma rede "interna" e a Internet uma rede "externa", podemos dizer que o Proxy é quem permite que outras máquinas tenham acesso externo.

Geralmente, máquinas da rede interna não possuem endereços válidos na Internet e, portanto, não têm uma conexão direta com a Internet. Assim, toda solicitação de conexão de uma máquina da rede local para um computador da Internet é direcionada ao Proxy, este, por sua vez, realiza o contato com o computador desejado, repassando a resposta à solicitação para a máquina da rede local. Por este motivo, é utilizado o termo Proxy para este tipo de serviço, que é traduzido para procurador ou intermediário. É comum termos o Proxy com conexão direta com a Internet.

Web Proxies

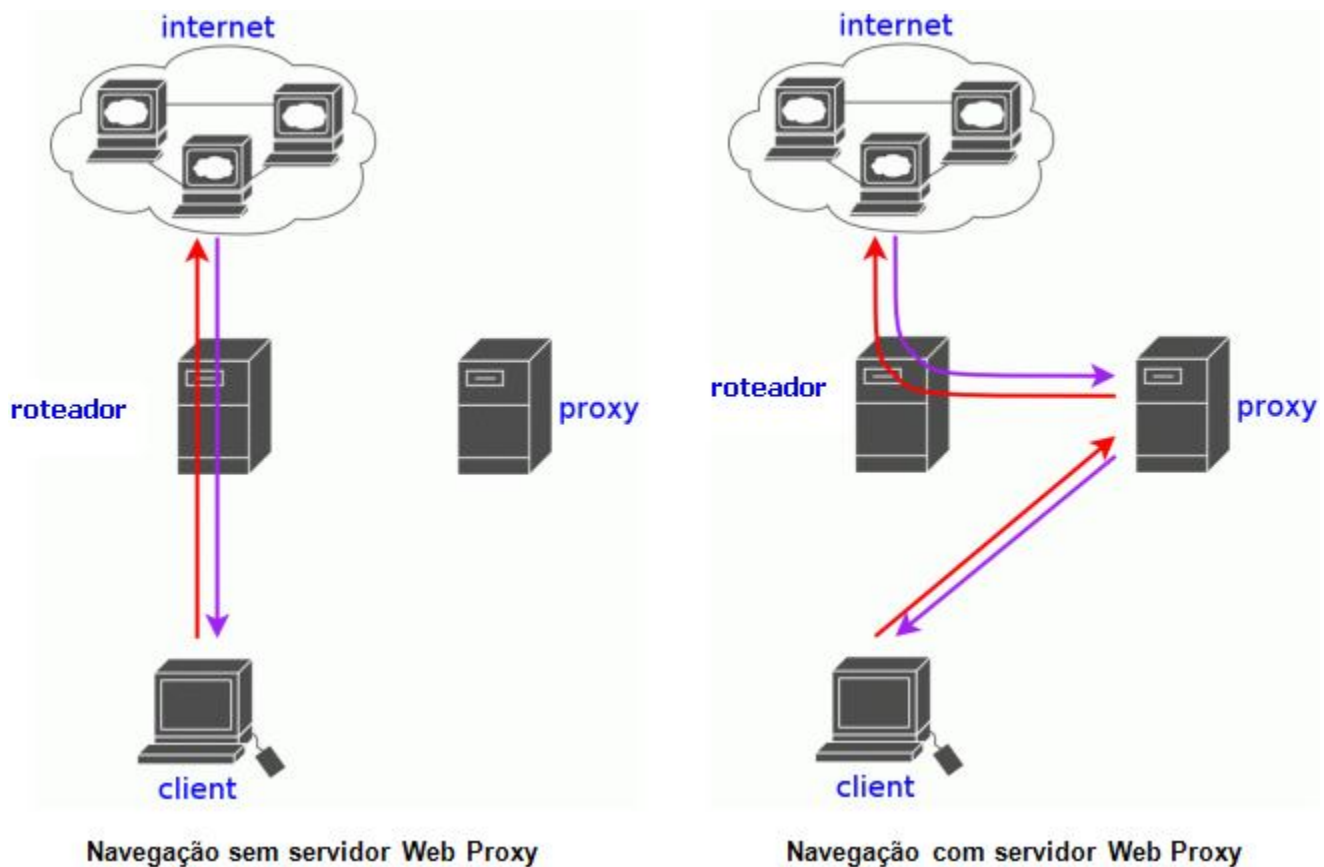
Uma aplicação Proxy popular é o **HTTP caching Web Proxy**. Este provê um cache de páginas da Internet e arquivos disponíveis em servidores remotos da Internet, permitindo aos clientes de uma rede LAN acessá-los mais rapidamente e de forma viável. Quando este recebe uma solicitação (de um cliente) para aceder a um recurso da Internet (especificado por uma URL), um Proxy que usa cache procura por resultados desta URL no seu cache local. Se o recurso for encontrado, ele é retornado imediatamente. Senão, ele carrega o recurso do servidor remoto, retornando-o ao solicitador e armazena uma cópia deste no seu cache.

O cache usa normalmente um algoritmo de expiração para remover documentos do cache, de acordo com a sua idade, tamanho e histórico de acesso. Dois algoritmos simples são o

Least Recently Used (LRU) e o Least Frequently Used (LFU). LRU remove os documentos que passaram mais tempo sem serem usados, enquanto o LFU remove documentos menos frequentemente usados. O Proxy também é usado por hackers, para navegar anonimamente, ou, é feita a substituição de um Proxy por outro, a fim de burlar proteções oferecidas pelo Proxy original.

A privacidade de servidores de Proxy públicos foi questionada, após um adolescente norte-americano de treze anos descobrir, através da análise do código fonte de um site, que um famoso site para navegação anônima, gerava logs com dados reais de seus usuários e os enviava para a policia norte-americana.

Navegação sem servidor Web Proxy

Navegação com servidor Web Proxy

Proxy Transparente

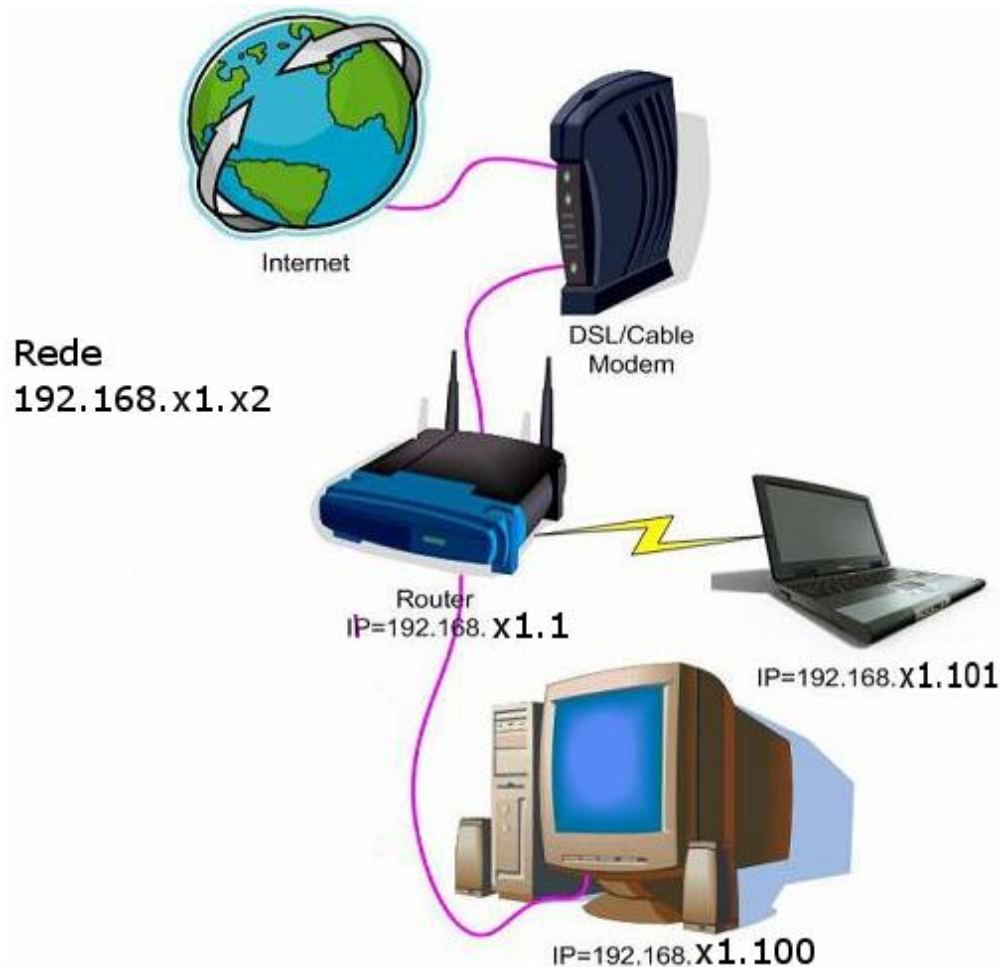
Um Proxy transparente é um método para obrigar aos usuários de uma rede a utilizarem o Proxy. Além das características de caching dos Proxies convencionais, estes podem impor políticas de utilização ou recolher dados estatísticos, entre outras. A transparência é conseguida interceptando o tráfego HTTP (por exemplo) e reencaminhando-o para o Proxy mediante a técnica ou variação de **Port Forwarding**. Assim, independentemente das configurações explícitas do usuário, a sua utilização estará sempre condicionada às políticas de utilização da rede. O RFC 3040 define este método como Proxy interceptador.

Dicas De Segurança Para Redes Home Wireless

O tópico de segurança em redes Wireless, sejam estas implementadas em casa (Home) ou no, é um assunto delicado, tanto pelos usuários da tecnologia, quanto pelos fabricantes de equipamentos. Segurança, apesar de ser um item fundamental em qualquer projeto de rede, ainda não é tratada como deveria ser por aqueles que estão montando uma pequena rede. Apesar dos recursos de segurança atuais não serem 100% invioláveis, é sempre bom garantir, ao máximo, que o ambiente de rede e possíveis dados de usuários estejam protegidos da melhor forma possível.

Segurança é o “calcanhar de Aquiles” das tecnologias Wireless, principalmente o Wi-Fi. Se já era difícil garantir e proteger redes convencionais de invasores, imagine como é conseguir que informações voando pelo ar, de um lado para outro, sejam protegidas de pessoas mal-intencionadas. Pensando dessa forma, todas as medidas de segurança, mesmo que simples, são bem-vindas.

Qualquer pessoa, sem muito conhecimento avançado sobre o assunto, pode adotar medidas básicas para melhorar a segurança de uma rede Wireless, o que muitas vezes acaba não acontecendo, criando assim, um verdadeiro paraíso para curiosos e intrusos, geralmente conhecidos como Hackers ou Wardrivers. Portanto, para dificultar a vida a todas aquelas pessoas que querem acessar à sua rede particular sem ser convidados e se proteger ao

máximo de invasões indesejadas mantendo pessoas estranhas longe dos seus arquivos, dados, projetos, você pode tomar algumas precauções como explicadas a seguir.

Primeiramente antes de iniciar a instalação da sua rede particular Wireless em casa verifique que o roteador (que você irá comprar) tenha como mínimo suporte a tecnologia 802.11g a 54 Mbps. Deve-se considerar também que o roteador possua as seguintes características:

- Filtragem por endereços físicos MAC Address;
- Wi-Fi Protected Access (WPA/WPA2);
- Firewall incorporado;

- DHCP Server;
- Configuração (interface) em formato Web para poder configurar as características do rotador utilizando um Browser (IE, Firefox, Opera, etc.)

Recomenda-se sempre ter uma conexão de banda larga (ADSL) e seguir os seguintes passos na configuração do seu modem:

- **Habilite e configure a encriptação de dados**: Utilizar a encriptação de dados é a melhor coisa que você pode fazer para começar a melhorar sua segurança. O método de encriptação mais comum é o WEP (Wired Equivalent Privacy), que lhe permite criar chaves de 64, 128 ou 265 bits. Outros métodos, como o WPA (Wi-Fi Protected Access), podem também ser utilizados, sempre levando em consideração que a encriptação, apesar de ser um item fundamental, não é a garantia de uma rede impenetrável. O novo protocolo Wi-Fi 802.11i especificado pelo IEEE há pouco tempo, além das chaves convencionais, também traz o sistema AES (Advanced Encryption Standard) que demonstra ser um grande avanço no que diz respeito ao Wi-Fi e seu futuro. Sem dúvidas, uma rede com dados encriptados, provavelmente espantará 99% dos curiosos de plantão, já que a quebra de chaves de 256 bits ainda não é uma tarefa para qualquer um.
- **Defina um SSID (Service Set Identifier)**: O SSID é o nome do seu ponto de acesso, que equipamentos visitantes precisam saber para conectar-se a ele. Pontos de acesso costumam vir com SSIDs padrão. Nomes como Linksys, Default e 3Com são apenas alguns nessa longa lista. Um SSID padrão pode ser uma informação bastante útil para quem está tentando invadir uma rede Wireless, afinal, sabendo qual a marca e modelo de determinado aparelho, fica fácil arriscar e tentar encontrar o endereço de administração do aparelho, usuário e senha do mesmo. Um SSID padrão geralmente significa que a rede foi configurada por alguém com muita pressa e/ou pouco conhecimento.

- **Mude a senha de administrador do seu Hotspot**: Uma vez com o SSID padrão em mãos, é muito simples chegar ao endereço IP principal, através do qual é possível ter acesso ao módulo de administração do aparelho. Cada fabricante tem um padrão de endereços IP que é configurado de fábrica ou quando é dado "Reset" no aparelho, por isso é importante habilitar a senha do módulo administrador do seu roteador sem-fio. Com a senha habilitada, a vida de um possível invasor fica mais difícil e ele não poderá entrar facilmente no módulo de administração, conseguindo informações valiosas para quem está atacando. Mesmo assim, com recursos mais avançados, como monitoramento de pacotes Wireless ou" força bruta", por exemplo, um possível invasor ainda é capaz de conseguir acesso ao seu roteador ou demais computadores na rede.

- **Use filtros MAC**: Se possível, defina no roteador quais são os endereços MAC das máquinas autorizadas a se conectar (muitos roteadores permitem isso). Também limite o número de endereços IPs fornecidos pelo servidor DHCP do seu ponto de acesso.

- **Desligue o Broadcast do SSID**: O envio do nome SSID pelo sinal é bastante útil nos casos onde o acesso do ponto é aberto ao público, pois quem se conecta precisa saber o nome do SSID para efetuar a conexão. Em redes sem visitantes (apenas computadores que raramente mudam) é possível desligar o envio do SSID pelo sinal, informando manualmente esse nome aos dispositivos autorizados a conectar-se ao ponto. Dessa forma, um estranho pode até saber que a sua rede está ali, mas terá isso como um desafio a mais na hora de invadir o seu ambiente. Caso a sua opção de Broadcast de SSID esteja habilitada, o ideal então é mudar o nome padrão para algum outro.

- **Regule a intensidade do sinal**: Este talvez seja o ponto em que a maioria acaba por pecar ao instalar uma rede sem-fio. Alguns aparelhos permitem que você configure a força do sinal, reduzindo ao máximo os sinais que ultrapassam os limites físicos de seu ambiente, impedindo que ele chegue ao alcance daquele vizinho curioso. O ideal é ir abaixando o sinal aos poucos sempre testando o nível de intensidade nos vários

pontos da casa ou ambiente. Assim, você dificulta ao máximo uma invasão via rádio, já que a grande maioria dos curiosos de plantão não vai estar equipada com antenas direcionais de alto ganho.

- **Instale um Firewall**: Todos os pontos acima estão relacionados aos estágios a serem vencidos antes do invasor alcançar o seu computador. A instalação de um Firewall no computador (ou se possível no roteador) reforça ainda mais a segurança, impedindo o acesso de pessoas indesejadas, mesmo que elas tenham vencido todos os estágios anteriores. As mais conhecidos para o mercado doméstico são as soluções de segurança da Zone Alarm, McAfee e Norton.

- **Bloqueie portas e protocolos não utilizados**: Muitos roteadores sem-fio e/ou pontos de acesso vêm com Firewalls simples, que servem para filtrar protocolos, aplicações e números de portas perigosas e/ou não utilizadas pelos computadores que estão no ambiente de rede. Além desse tipo de precaução, você também poderá recorrer ao recurso de "Port Forwarding", para desviar certos tipos de requisições externas (Netbios, Telnet, echo, remote desktop, backdoor, etc), fazendo com que elas nunca cheguem aos computadores dentro da rede.

Conclusão Da Segurança Em Redes Home Wireless

Mesmo que você tome todas as precauções possíveis para proteger a sua rede sem-fio, nada impedirá que alguém monitore o sinal que trafega por ela, utilizando programas específicos e amplamente conhecidos. Para evitar ou dificultar isso, as poucas alternativas que sobram são o controle de intensidade do sinal (tanto do roteador, quanto dos clientes de rede) e a utilização de encriptação avançada, já que chaves do tipo WEP podem ser facilmente quebradas por quem realmente sabe aonde quer chegar.

Caso a sua rede Wireless precise de um nível de segurança maior que a alcançada através das medidas acima, isso indica que ela precisa ser projetada e implementada por profissionais capacitados. Redes para escolas, locais públicos, médias e grandes empresas,

condomínios, etc., precisam de atenção especial. O projeto de uma rede com tamanha importância ou proporções leva em conta fatores como clima e topografia, sendo uma tarefa para ser executada por empresas ou profissionais especializados.

UNIDADE 28

Objetivo: Saber como, quando, onde surgiu e qual o futuro desta grande rede.

Internet

A Internet originou-se da Arpanet, a primeira rede nacional de computadores criada em 1969 pelo Departamento de Defesa (DoD) dos Estados Unidos de Norte América para garantir a segurança em caso de acidente nas comunicações.

Esta rede privada era destinada a interligar os computadores dos centros de pesquisa, universidades e instituições militares americanas, permitindo o compartilhamento de recursos entre os pesquisadores que trabalhavam com projetos estratégico-militares.

Ela foi concebida pelo governo americano inicialmente com fins militares (como um recurso em caso de guerra), de tal maneira a ser um sistema robusto em manteria de comunicações, ou seja, mesmo que um nó central da rede seja destruído (por exemplo, Washington) as comunicações (entre os outros nós da rede) continuariam inalteradas. O próprio protocolo de roteamento teria a tarefa de reconfigurar as rotas disponíveis para contornar os nós desabilitados da rede.

Em 1972 o governo americano decidiu mostrar o projeto pioneiro à sociedade, e a ideia expandiu-se entre as universidades americanas, interessadas em desenvolver trabalhos cooperativos. Para interligar os diferentes computadores dos centros de pesquisa, em 1980 a Internet adotou o protocolo aberto TCP/IP para conectar sistemas heterogêneos, ampliando

a dimensão da rede, que passou a falar com equipamentos de diferentes portes, como micros, Workstations, mainframes e supercomputadores.

Somente em 1983, com a separação entre as aplicações para as áreas civis e militares, surgiu definitivamente o nome Internet. Três anos depois, a National Science Foundation criou uma ligação de alta velocidade com seu centro de supercomputadores e passou a promover a disseminação das informações científicas.

Naquela época, o governo americano decidiu financiar a formação de redes regionais em todo o país uma infraestrutura com circuitos dedicados e multiplexadores com canais do tipo T1 a 2 Mbps, o que acabou constituindo a NSFnet como uma via expressa para mandar mensagens e arquivos por todo o país. Essa rede, por sua vez, é conectada a outras redes comerciais e públicas que configuram a rede Internet, hoje o principal alicerce das comunicações entre os computadores mundiais.

Quem Manda Na Internet?

A razão porque a Internet funciona tão bem é porque (aparentemente) não existe um dono. A Internet é descentralizada, e um pouco anárquica. Não existe um organismo central encarregado da sua manutenção, nem responsável pelo estabelecimento de regras. Em vez disso, existe uma organização de usuários da Internet, chamada Internet Society ISOC (http://www.isoc.org). Esta organização é inteiramente composta por voluntários, e o seu único objetivo é promover uma troca universal da informação através da mesma tecnologia utilizada na Internet.

Os líderes desta organização, coletivamente chamados Internet Architecture Board (IAB), têm a responsabilidade de gerir tecnicamente e dirigir a Internet. Este grupo é responsável pela padronização da tecnologia utilizada para se ligar a, comunicar com, e trabalhar dentro da Internet. Estes padrões são desenvolvidos à medida que são necessários, através da contribuição de indivíduos interessados. Quem trata destes padrões é outro grupo do ISOC, conhecido como Internet Engineering Task Force IETF (http://www.ietf.org), que também é

composto por voluntários que estão interessados em resolver os problemas técnicos que a Internet enfrenta.

Quem Paga A Internet?

A Internet é paga pelas pessoas que a utilizam. As pessoas e empresas que estabeleceram a ligação à rede são responsáveis pela mesma. À medida que foram forjadas novas ligações, emergiu um sentido de responsabilidade partilhada. Não existe autoridade central ou entidade governamental responsável pela rede como um todo. Em vez disso, esta comunidade de redes individuais é coletivamente responsável pela rede.

O Que Se Pode Fazer Na Internet?

A Internet existe para fornecer uma livre partilha de informação, disseminar as suas conclusões, trocar ideias e conhecimentos ou falar com outros usuários, podendo mesmo colocar questões aos peritos mundiais.

Não existe uma estrutura formal na Internet. Um usuário pode simplesmente passear pela Internet, lendo comunicações públicas e copiando para o seu computador a informação de que necessita. Pode também contribuir com informação, tornando disponível o seu conhecimento e disponibilizando tempo para ajudar outros que possam ter questões ou problemas.

Utilizando a Internet pode-se encontrar informação sobre virtualmente qualquer tópico imaginável, desde a Arqueologia até à Zoologia. Pode pesquisar informação relacionada com uma investigação que está a realizar, informar-se sobre a evolução dos mercados financeiros ou mesmo encomendar uma pizza.

Os americanos dão a este conceito o nome de “information at your fingertips”, ou seja, a informação na ponta dos seus dedos. O problema muitas vezes é localizar a informação. Não existe um depósito de dados da informação pretendida, nem existe um índice que indique

onde é que ela está localizada. Existem, porém ferramentas que o ajudam na sua pesquisa, tais como os motores de busca, por exemplo, Yahoo.com, Google.com, Altavista.com, etc.

A maior parte dessa informação é gratuita, estando disponíveis na Internet vários milhões de documentos. Além disso, existem milhares de arquivos que contêm documentação técnica sobre os mais diversos assuntos, jogos, programas de multimídia, demonstrações de programas comerciais e mesmo imagens, vídeos e sons que se pode utilizar livremente.

Os informáticos têm na Internet um verdadeiro tesouro de informação e de programas. Ela é utilizada para obter software gratuito e distribuir atualizações (Upgrades) de software, além dos inevitáveis relatórios e correções de erros (Bugs). Serve também como serviço de suporte técnico, permitindo a alguém que tenha um problema, colocar a sua questão em um Newsgroup e obter uma resposta pouco tempo depois.

Utilidade Da Internet

A Internet possibilita que milhões de pessoas separadas por distancias geográficas enormes conversem horas a fio teclando suas frases nos computadores e pagando o preço de uma ligação telefônica local. Serve para consultar um livro ou um documento em 2.000 bibliotecas que podem ser acessadas a distância, 24 horas por dia. É melhor ler Guerra e Paz, o romance épico de Tolstoi num livro convencional. Mas que tal quando se trata de levantar informações sobre o próprio Tolstoi ou sobre religiões hindus? Uma consulta dessas não demora mais de meia hora. Centenas de bibliotecas ao redor do mundo podem ser rastreadas automaticamente em busca da informação desejada.

A Internet serve também para que as pessoas com interesses comuns, como ecologistas, os médicos ou os fanáticos por esportes, conversem com suas almas gêmeas espalhadas pelo mundo. Serve para que cientistas separados no tempo e no espaço possam trabalhar em

projetos comuns, compartilhando uma mesma tela, mas usando teclados diferentes, um deles em Paris e o outro em Nova York. Adeus aos telefonemas internacionais a preço de caviar ou a falta de informações só porque se vive numa cidade provinciana. Adeus para as conversas maçantes com vizinho quando se tem disponível o mundo inteiro para se bater papo.

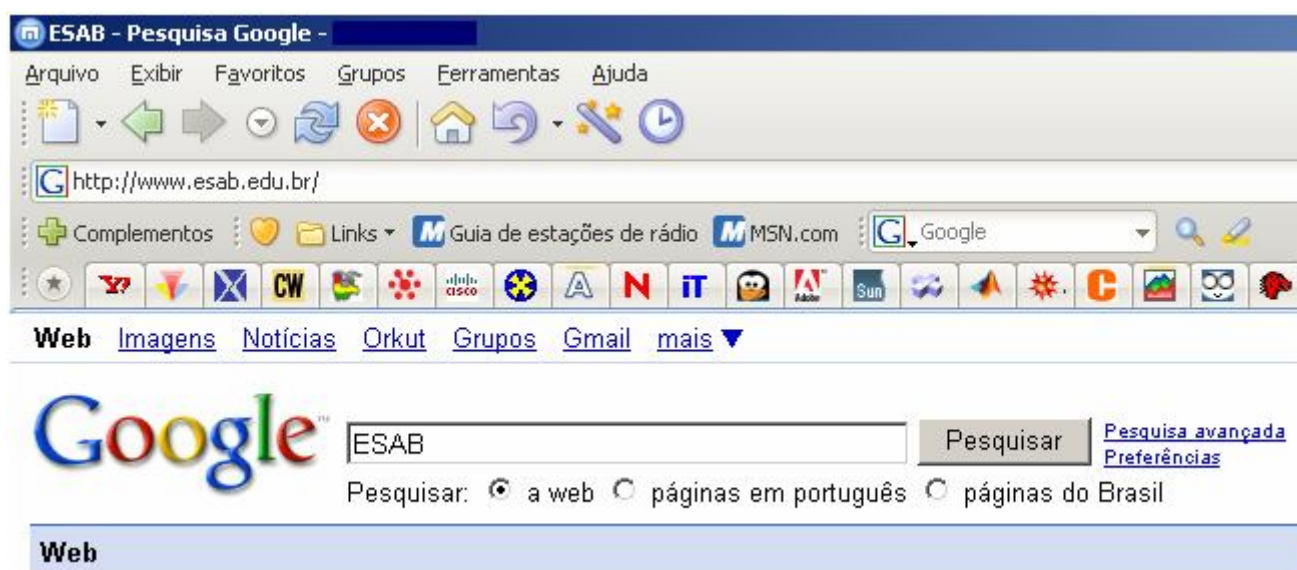
Também se pode flertar verbalmente pela Internet. Faz-se muito esse esporte. Briga-se também. E vale soltar palavrão, procedimento comuníssimo na rede. Pode servir também para dar uma olhada gulosa em centenas de imagens de alta qualidade das pinacotecas do Vaticano e da Instituição Smithsoniana, em Washington. Ou para montar a mais fabulosa coleção de imagens pornográficas cujas reproduções digitais trafegam pela rede sem censura.

A partir de meados da década dos 90, a Internet iniciou a sua explosão comercial. Poderíamos dizer que foi neste ponto o início da era das empresas do tipo **.COM** cada uma delas mostrando seus produtos e fechando negócios através do computador ou (como é muito utilizado hoje em dia) On-line.

No final dos anos 90 foram publicados dois anúncios nos EUA mostrando como está a velocidade das mudanças no espaço cibernético. O cartão de crédito Visa anunciou ter desenvolvido um programa de cobranças que permite lançar valores mínimos de até 31 centavos de Dólar - o que abre espaço para venda de selos, chocolates e outras bugigangas que não tinham peso econômico para virar ofertas numa rede de computadores. "Trinta e um centavos parecem uma gota no oceano, mas, quando se imagina que a rede terá brevemente 100 milhões de usuários, essa gota poderá vir a ser o próprio oceano", diz David Melancon, diretor do cartão Visa. No outro extremo, Gary Whitaker, revendedor de automóveis Rolls-Royce em Beverly Hills, na Califórnia, comunicou que passará a anunciar na Internet, onde já estão nomes populares, tais como, Pizza Hut, a General Motors, Boeing, Microsoft, etc.

Não é apenas por ostentar números grandiosos que a Internet é um fenômeno. Tampouco por permitir o acesso a textos de bibliotecas e a reproduções de quadros famosos dos

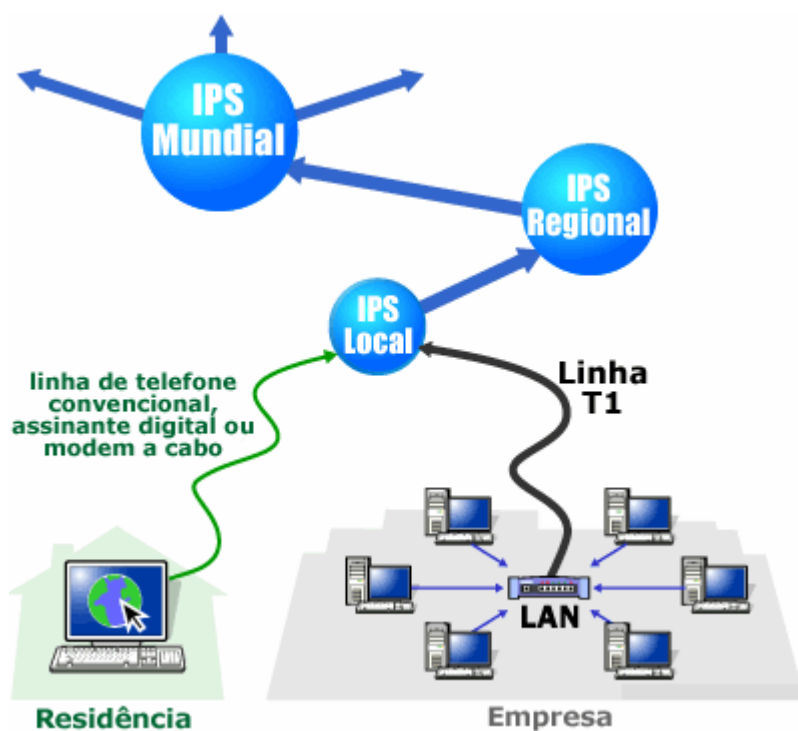
grandes museus, como o Louvre, de Paris. Nem pelos avanços tecnológicos criados com a operação da rede. Mais que tudo isso, a Internet é uma experiência humana rara, é a concretização da profecia da aldeia global.

Em cada época, surge um grupo de inovações que toma conta da indústria e marca o ritmo de toda a sociedade. Os anos 90 estão entregues à alta tecnologia, a indústria de informação e de transformação digital. Que se define pelo poder de empacotar todas as informações culturais na forma de bits, a menor unidade de informação na linguagem dos computadores. Canções podem ser digitalizadas - como já são nos CDs musicais - e, assim passeiam pela Internet. Jornais inteiros são igualmente transformados em bits e postos à disposição de assinantes. Dinheiro pode também trafegar como mensagem cibernética, na forma de números de cartão de crédito.

A Internet carrega essa riqueza com muita eficiência. A rede tem basicamente três tipos de computadores interligados. Os do primeiro tipo são computadores servidores, grandes fornecedores de informações e programas. Em geral pertencem a uma universidade ou instituição de pesquisa, ou então a uma grande empresa que estoca nele uma descrição de seus produtos. Os do segundo tipo são os nódulos, grandes máquinas que agem como servidores, mas também ajudam a escoar o tráfego de informações na rede. Os

computadores do terceiro tipo, mais numerosos, são os dos usuários, nós, que estamos na rede para receber e não para dar. É claro que os receptores estão longe de ser passivos. Passam mensagens, entram em discussões, cravam pontos de vista sobre isso ou aquilo. E uma página de texto colocada por qualquer membro da Internet pode ser lida por milhões de pessoas.

A Internet No Brasil

O Brasil tem muitos usuários conectados à Internet e cada dia esse número de Internautas cresce. O interesse pela Internet no país ultrapassou os limites acadêmicos e chegou a todos os usuários de computadores. A demanda é tanta que a Embratel decidiu oferecer, a partir de dezembro de 94, acesso comercial à maior rede de informações do mundo. A empresa criou um serviço que dará a seus clientes acesso on-line as bases de dados de todo o mundo, com informações de interesse geral como esportes, eventos, espetáculos, previsão meteorológica e sinopses de periódicos. O serviço permitirá também a realização de conferências eletrônicas.

O serviço iniciou-se pela Renpac (Rede Nacional de Pacotes) e pelo serviço de Caixas Postais Eletrônicas STM-400 da Embratel e atualmente pode ser acessado tanto por grandes corporações de muitos computadores assim como por usuários domésticos com apenas um micro pessoal. O acesso será transparente para usuários do STM-400, explica o coordenador do projeto, Hélio Dalgegan, assessor da

presidência da Embratel. A empresa vai adotar o correio eletrônico da Internet e já está convertendo o protocolo SMTP, que permitirá acesso direto à rede mundial. "O processo comercial muitas vezes envolve valores e dados comerciais que são confidenciais e, por ser muito aberta, a rede não oferece nenhuma garantia de confiabilidade e codificação de dados". Vendo o sucesso da Internet, a Embratel assume o comando das ligações de brasileiros com a rede.

Era dezembro de 1994, mudanças a vista. A primeira, o governo americano privatizava o último tronco de fibras ópticas de alta velocidade da Internet que ainda mantinha em seu poder. A segunda, a estatal brasileira Embratel anunciava a fase de testes do primeiro serviço nacional de acesso a Internet.

O poder público americano lançou as bases de comunicação da rede, financiou (durante os primeiros anos) e subsidiou a sua manutenção até faz pouco tempo. Quando concluiu que poderia andar sozinha, sem a mão pesada do governo, Washington desligou-se da Internet. Já o governo brasileiro como tudo o que faz, fez novamente o contrário. A Embratel deu as costas para a Internet em seus primeiros anos, deixando que os poucos usuários brasileiros, principalmente universidades e institutos de pesquisa tomassem a iniciativa de contratar suas conexões no exterior. Agora a rede começa a ter viabilidade, a Embratel anuncia que está no negócio. Sozinha. A conexão é monopólio da Embratel. No Brasil a Internet acaba de tornar-se mais um departamento da Embratel. Embora os custos de conexão, ao longo dos anos, foram diminuindo o acesso em banda larga (alta velocidade) ainda é um tanto caro para os usuários brasileiros.

A Web 2.0

O conceito de Web 2.0 representa a segunda geração de várias comunidades e serviços na Internet, como por exemplo, redes sociais de sites (Wikipedia, Youtube, Hi5, Flickr, Facebook etc). O objetivo principal destas redes é o de facilitar a colaboração e troca de informação entre todos os usuários e os sites e serviços virtuais contribuindo para uma maior interacção

com a Internet e para a organização do seu conteúdo. O termo ganhou alguma popularidade numa conferência anual organizada pela O'Reilly Media em 2004, Web 2.0 Conference.

Embora a palavra remeta para uma nova versão da Internet, esta não representa nenhuma atualização técnica na rede, mas sim, uma alteração na forma como os programadores e usuários a abordam atualmente.

Nos últimos anos, o termo tem estado na origem de debates, artigos, livros. Embora existam algumas divergências e tendo sido feitas inúmeras projeções e previsões acerca do destino da Web 2.0, este novo conceito é hoje em dia ponto assente entre a comunidade.

Acontece que a Internet veio para ficar e já têm um público maior que os jornais, as revistas e TV por assinatura. Apesar disso, ainda há uma resistência do mercado em anunciar na internet, o que é um erro, já que grande parte das pessoas procura na Web a referência sobre o que desejam consumir.

Com a Web 2.0, as ferramentas de busca são de grande importância para o novo cenário do marketing na rede, porque ela possibilita que o usuário chegue exatamente no resultado que demanda.

Hoje está cada vez mais difícil alcançar os consumidores porque eles estão mais fragmentados. Isso remete ao conceito que o Google denominou de Lovecasting, que é a ideia de que a Internet permite ao usuário acessar apenas o que lhe interessa, diferente do Broadcasting e do Nerocasting. Neste sentido, o marketing na Internet também precisa estar direcionado para este conceito, e por esta razão, as buscas são uma importante ferramenta

de marketing. Nesta nova etapa, a expectativa é de que consigamos superar a primeira etapa, na qual tentamos desesperadamente encaixá-la em todos os modelos conhecidos de comunicação. Basicamente, um emissor divulgando informações e tantos outros as recebendo. Quando os primeiros usuários entraram na rede começaram a perceber que este modelo clássico poderia ser modificado e diversos visionários criaram produtos e serviços, que foram aos poucos mostrando este novo potencial.

Entre esses potenciais estão os primeiros navegadores que permitiam a leitura de textos, alias de hipertextos, de forma anárquica, através de hiperlinks, e não mais na ordem de um livro tradicional, página a página. As listas de discussão e os grupos eletrônicos que possibilitaram o primeiro modelo de uma comunicação colaborativa, sem a figura do emissor único. O correio eletrônico que permitiu a troca de mensagens, barata e a longa distância para múltiplos destinatários. Os mensageiros eletrônicos que expandiram o conceito da comunicação virtual para uma presença constante e troca de pequenas mensagens entre amigos e colegas de trabalho ao longo do dia e das madrugadas.

E a evolução permanente dos Websites, que foram aos poucos permitindo cada vez mais a participação e a colaboração dos usuários no processo de geração de informação. Na verdade, a expectativa da Web 2.0 é criar alguns novos paradigmas.

A Internet é um novo meio de comunicação, com forte tendência à interação. Ou se quisermos ser mais radicais: a Internet é um meio de interação, com uma forte possibilidade de comunicação horizontal. Assim, a Web 2.0 tem como proposta passar a limpo os experimentos e erros de adaptação do modelo de comunicação clássica para este novo ambiente, que continuam por aí, mas diminuindo gradualmente.

Assim, quando falarmos de Web 2.0 estamos partindo do princípio que os agentes deste processo estarão trabalhando na tentativa de potencializar ao máximo este novo ambiente:

tendo a colaboração, a interação e a força do coletivo, como o motor para dar respostas a essa nova sociedade virtual.

Ou seja, quanto mais virtualizamos a sociedade, mais rápida ela gera seus ciclos e mais depressa precisamos acompanhá-los para tomar as decisões, que vão da escolha da carreira do filho ao investimento de bilhões de uma nova fábrica.

É preciso encarar esta fase como uma segunda fase da Internet, em que os investimentos serão ponderados, os modelos de negócios terão bases sólidas e em que todos teremos muito a ganhar.

Atividades

Atividade Dissertativa

Evolução da Internet: da DARPANET à Internet atual

Comprimento: duas folhas (no mínimo)

UNIDADE 29

Objetivo: Saber quando é possível implantar uma Intranet em uma empresa.

Intranet

Como consequência do desenvolvimento tecnológico tanto em hardware como em software assim como o desenvolvimento de protocolos de comunicação é que aos poucos fez seu aparecimento uma das maravilhas modernas chamada de Internet. Na metade da década dos 90 surgiu o conceito de Intranet, é bom mencionar que essa ideia de Intranet vem quase conjuntamente com a explosão comercial (não mais militar nem científica) da Internet, e a aceitação dessa ideia pegou muito bem, sobre todo, nas Corporações do mundo todo.

A Internet é a “novidade” mais útil (se é que ainda pode ser chamada de novidade), consistente e acessível que a informática nos trás. São milhões de computadores interligados em todo o mundo, o acesso é fácil e imediato, as informações se apresentam em formato gráfico e agradável.

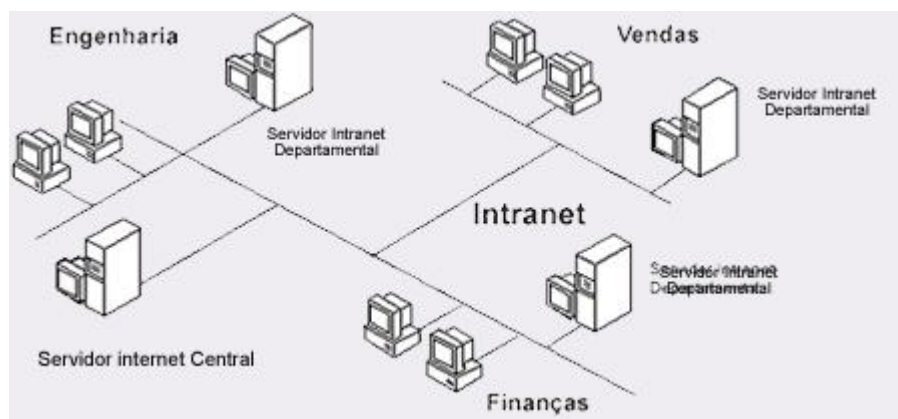
Nela é possível que qualquer pessoa ou empresa procure ou forneça informações. Pode-se afirmar que uma empresa poderá dispor seus dados na Internet pelo mesmo custo e com a mesma qualidade que uma pessoa qualquer, É bom e barato.

Atualmente, quem acessa a Internet, conhece o seu lado popular, sites sobre lazer, shopping, esporte, cultura, etc. As Intranets têm a ver com os sistemas corporativos de informações, que também podem ser acessados via Internet. As empresas descobriram que

podem criar redes como a Internet, porém privadas, as Intranets, que cumprem o papel de conectar entre si filiais, departamentos, fornecedores, clientes, etc.

Mesclando (com segurança) as suas redes particulares de informação com a estrutura de comunicações da Internet. As oportunidades de modernização operacional são incontáveis.

Enquanto a Internet estabelece os padrões e as tecnologias para comunicação entre computadores, através de uma rede mundial que conecta muitas redes, a Intranet aplica estas tecnologias dentro da organização via a rede LAN/WAN corporativa, com todos os mesmos benefícios. Exatamente pela Internet ser um padrão bem estabelecido, montar a infraestrutura é simples. O clássico problema de como fazer um se conectar com muitos é resolvida pelo uso da tecnologia Internet via WAN/LAN. O controle de acesso e segurança, problema complicado nos modelos informacionais atuais também encontramos solução nos moldes da Internet.

A tecnologia da Internet passa a se incorporar na nova logística empresarial de fora para dentro, ou seja, para suportar toda essa nova dinâmica externa a logística interna precisa acompanhar, a questão básica é: a empresa quer responder pronta e corretamente às demandas pelo seu canal de vendas e seus parceiros. Não dar respostas, seja por telefone ou Internet é igualmente inadmissível. Portanto, já é hora de começar a operar via Internet, aos poucos, sempre conscientes de que a essência do sucesso operacional neste novo cenário passa, aos poucos, por uma integração de todos os sistemas computacionais desde o nível de simples coleta de dados até a apresentação multimídia via Internet.

É ponto pacífico que apoiar a estrutura de comunicações corporativas em uma Intranet dá para simplificar o trabalho. Embora seja cedo para se afirmar onde realmente a Intranet vai ser mais efetiva para unir, no sentido operacional, os diversos profissionais de uma empresa. Isto se deve as dificuldades de tirar informação de um lugar e disponibilizar para todos os interessados, as empresas replicam esforços em diversas áreas e, na falta de unicidade de informações, as decisões tomadas em áreas diferentes, mas inter-relacionadas, são muitas vezes conflitantes.

A Intranet é a melhor ferramenta para disponibilizar a representação de uma mesma realidade para muitas pessoas, superando as dificuldades acima. E é exatamente por isso que ela se estabelece como uma explosão de remodelamento empresarial e se transforma tão rapidamente, de um sistema de integração pública, a uma estratégia de comunicação corporativa. Para superar os problemas de comunicação corporativa a Intranet apresenta uma estrutura de comunicações ONIPRESENTE, qualquer um se comunica de qualquer lugar para qualquer lugar.

Os canais de comunicação também variam, um canal dedicado de alta velocidade atende a um tipo de demanda (por exemplo: atualização constante de dados entre fábricas e depósitos), canais de acesso compartilhado (por exemplo: vendedores espalhados pelo país, consultando a nova tabela de preços) caracterizam um acesso não tão constante, mas geograficamente disperso e variado.

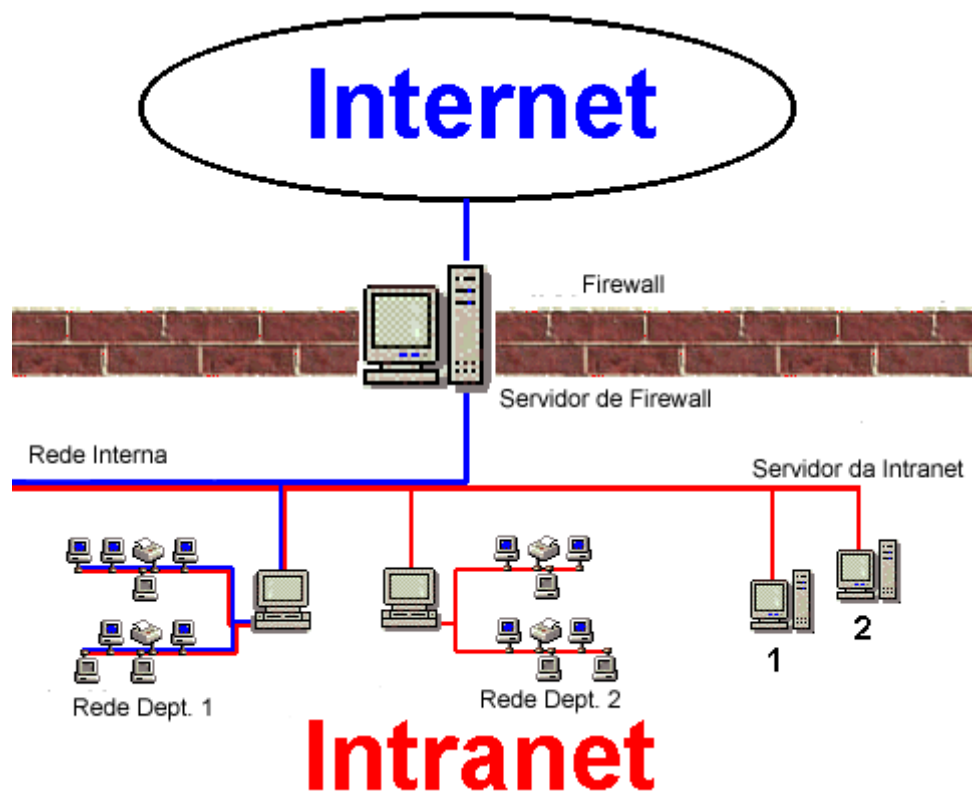
A Intranet vai usufruir dos dois canais, sem problemas, e os usuários não vão ter problema de usar a Intranet ou a Internet, porque são dois nomes para a mesma coisa, ninguém percebe se o canal de comunicação é público ou privado. Um diretor vai olhar o mesmo gráfico de vendas, ou consultar uma promessa de entrega, no computador da sua mesa, no meio da fábrica ou de casa.Enfim, ele vai entrar na sua Intranet a partir de qualquer lugar, via Internet.

A Internet possui uma inovação conceitual, onde a informação não é mais enviada, mas sim buscada sob demanda. Não se enviam mais catálogos, listas de preços, promoções, mensagens, todos passam, a saber, onde estas informações estão disponíveis e as buscam

sempre que precisam. Isto simplifica radicalmente muitas coisas, principalmente no que tange aos procedimentos de atualização e geração de informações, não se imprime coisas a mais nem a menos, simplesmente porque não se imprime mais nada.

Para se montar uma Intranet, devido às ferramentas já disponíveis, será um processo técnico relativamente simples. Mas como dito anteriormente o problema maior na implementação de uma Intranet está no fato de ser necessário alterar o modo de operação e a logística das corporações, enfrentando tarefas como a aculturação de executivos, remodelamentos operacionais, renovação de ambientes computacionais, etc.

A Intranet é sem dúvida nenhuma a nova onda da organização empresarial utilizando-se da informática a fim de se obter uma maior produção e agilidade no fornecimento de informações e atendimento as necessidades.

Podemos resumir que a Intranet em uma empresa é a responsável por garantir a comunicação interna e a coerência das informações, com velocidade e total segurança dentro da empresa, sem o risco de violação por "pessoas não autorizadas".

UNIDADE 30

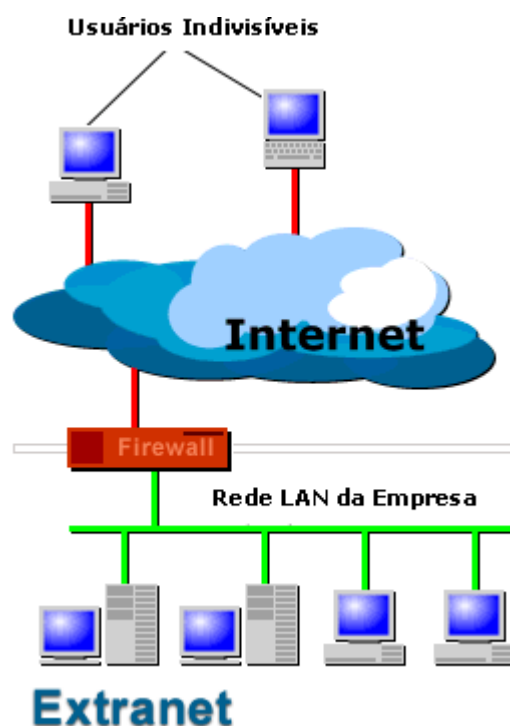
Objetivo: Entender o funcionamento do conceito de Extranet na atualidade.

Extranet

Extranet é a tecnologia usada para interligar várias Intranets. A extranet, também chamada de **B2B** (Business to Business, ou negócios entre empresas via Internet) é uma intranet que se projeta ao meio externo com acesso controlado, geralmente entre o cliente e a empresa. O acesso pode ser feito através do site, a partir de qualquer máquina conectada à Internet.

Uma Intranet pode utilizar-se da infraestrutura de comunicações da Internet para se comunicar com outras Intranets (por exemplo, um esquema de ligação matriz-filial). É possível disponibilizar qualquer serviço para o cliente oferecendo comodidade e acesso 24 horas e, é claro, com total segurança. Independente da posição geográfica entre a empresa e o cliente, o custo operacional é muito pequeno.

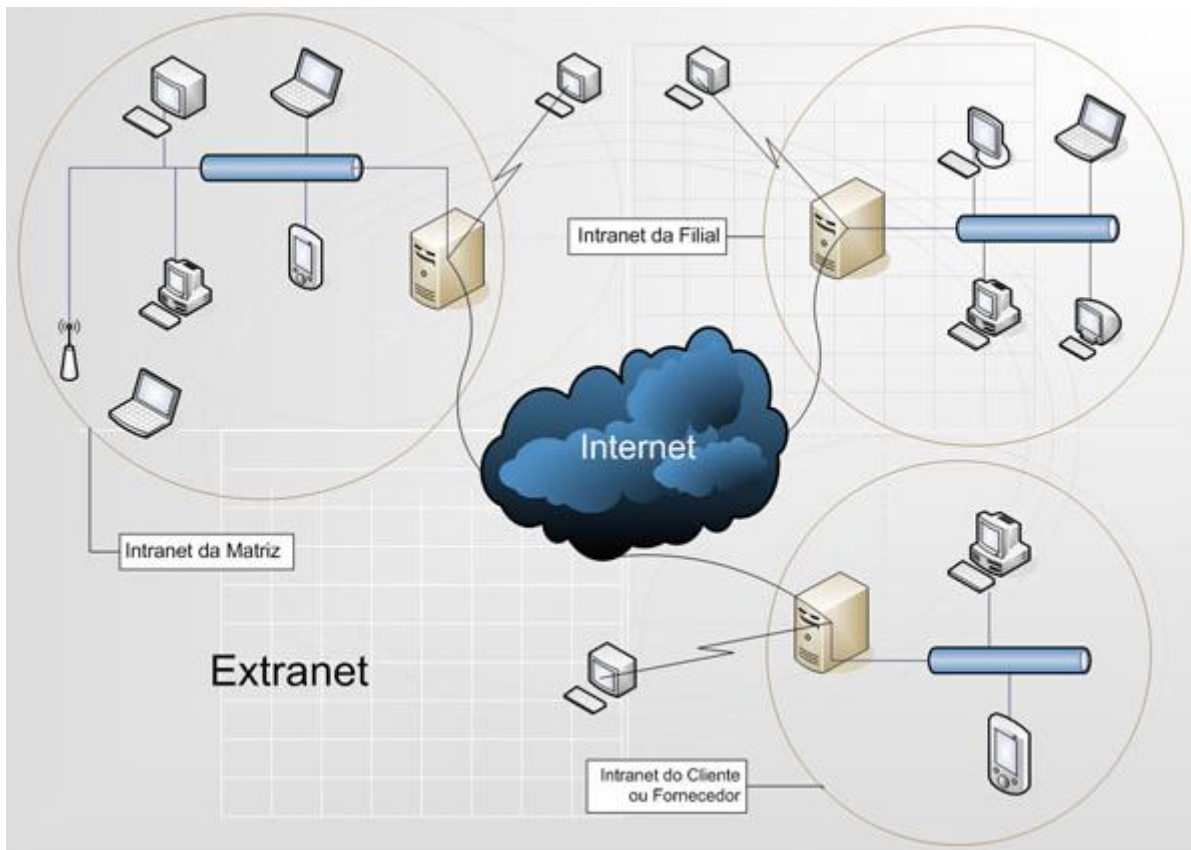
Portanto, para a pergunta "Quais são as condições para criar uma Extranet?" Temos a seguinte resposta. Quando se necessita disponibilizar informações corporativas que não são de domínio público a clientes e parceiros seletos, então isto não é mais função da Intranet, mas sim da Extranet.

Este termo que veio à tona com a evolução da Internet/Intranet surgiu como o meio que permite que as companhias troquem informações. É a parte da Intranet que os clientes e fornecedores podem acessar. Na essência, o conceito encerra a ideia de estender a Intranet,

por meio de Links extras, para acesso de parceiros de negócios, sejam clientes, revendas, distribuidores, fornecedores ou prestadores de serviços.

Os clientes e estes parceiros de negócios têm acesso a tais informações (geralmente armazenadas em bancos de dados criados especialmente para esse fim) através de Login e senha, e suas visitas são registradas e acompanhadas pelo servidor. A segurança para a transmissão de informações sigilosas, como o número do cartão de crédito, por exemplo, também tem que ser garantida.

- Uma Extranet é um site de internet que apenas está acessível a um selecionado grupo de pessoas (usuários indivisíveis).
- Uma Extranet disponibiliza uma forma de se criarem aplicações que parceiros e clientes podem aceder, mas que não estão acessíveis eo público em geral.
- Extranets podem usar encriptação e palavras-passe para assegurar o acesso ao site apenas por quem for autorizado.
- Para transações B2B, as Extranets proporcionam o comércio eletrônico seguro.
- Uma Extranet pode automatizar a partilha de informação ao providenciar acesso a informações específicas e acesso controlado a bases de dados internas.

Em resumo, uma Extranet garante a comunicação entre a empresa e o "mundo exterior". Esta comunicação segura acontece em tempo real, e pode contar com tipos de acesso diferenciados como, por exemplo, para: fornecedores, funcionários, ou vendedores (que passam a maior parte do tempo fora da empresa). Estas informações são interligadas aos sistemas internos da empresa (ERP, CRM, etc.), para garantir que todas estejam sempre atualizadas.

Extranet é o nome dado a um conjunto de Intranets interligadas através da Internet. É uma rede de negócios que une empresas parceiras por meio de suas Intranets, utilizando os padrões abertos da Internet.

Esses parceiros não precisam ter o mesmo tipo de computador (hardware), sistema operacional, gerenciadores de banco de dados (softwares) ou Browser para navegação.

- A Extranet amplia ou estende os benefícios de uma Intranet para parceiros de negócios.
- A Extranet liga os interesses da organização com seus parceiros de negócios.
- A Extranet cria um senso de comunidade com os seus parceiros de negócios.
- A localização de uma Extranet depende, em parte, das conexões de acesso.

Atividades

Antes de dar início à sua Prova Online é fundamental que você acesse sua SALA DE AULA e faça a Atividade 3 no "link" ATIVIDADES.

GLOSSÁRIO

1Base5 - Ethernet de Par Trançado sem blindagem; velocidade de 1 Mbps; a distância máxima entre estações de trabalho e o conector é de 500 metros. Não muito utilizado.

10Base2 - CheaperNet, ThinNet ou Thin Ethernet; velocidade de 10 Mbps; o segmento máximo de cabo é de 200 metros.

10Base5 - Ethernet espesso, o sistema de cabo especificado pela Dec e Xerox; velocidade de 10 Mbps; o segmento máximo de cabo é de 500 metros.

10Base-F - Ethernet de Fibra; utilizado entre estações de trabalho e um concentrador; velocidade de 10 Mbps; a distância estimada é de 2,2 quilômetros.

10BaseT - Ethernet de par trançado; velocidade de 10 Mbps. Muito popular.

Agente - Um programa de computador ou processo que opera sobre uma aplicação cliente ou servidor e realiza uma função específica, como uma troca de informações.

Alias - Significa segundo nome ou apelido. Pode referenciar um endereço eletrônico alternativo de uma pessoa ou grupo de pessoas, ou um segundo nome de uma máquina. É também um dos comandos básicos do UNIX.

ANSI - Acrônimo de American National Standards Institute, uma organização afiliada à ISO e que é a principal organização norte-americana envolvida na definição de padrões (normas técnicas) básicos como o ASCII.

Anatel - A Agência Nacional de Telecomunicações (Anatel) é uma autarquia brasileira, administrativamente independente, financeiramente autônoma, não subordinada hierarquicamente a nenhum órgão de governo brasileiro. Por ser uma Autarquia, é uma entidade auxiliar da administração pública descentralizada, tutelada pelo estado Brasileiro, e fiscalizada pela população.

Aplicação - Programa que faz uso de serviços de rede tais como transferência de arquivos, login remoto e correio eletrônico.

Archie - Um serviço de busca de arquivos armazenados em FTP anônimo. Pouco disseminado no Brasil.

ARPANET - Advanced Research Projects Agency Network. Rede de longa distância criada em 1969 pela Advanced Research Projects Agency (ARPA, atualmente Defense Advanced Projects Research Agency, ou DARPA) em consórcio com as principais universidades e centros de pesquisa dos EUA, com o objetivo específico de investigar a utilidade da comunicação de dados em alta velocidade para fins militares. É conhecida como a rede-mãe da Internet de hoje e foi colocada fora de operação em 1990, posto que estruturas alternativas de redes já cumpriam seu papel nos EUA.

ASCII – É a sigla da American Standard Code for Information Interchange. Trata-se de um esquema de codificação que atribui valores numéricos às letras do alfabeto, números, sinais de pontuação e alguns símbolos especiais para ser usado em computadores e dispositivos de armazenamento eletrônico de dados.

Assinatura - 1. Um arquivo (tipicamente de três ou quatro linhas) que as pessoas inserem no fim de suas mensagens; 2. Ato de subscrever uma lista de discussão ou newsgroup; 3. Informação que autentica uma mensagem.

ATM Protocolo de Modo de Transmissão Assíncrona de Dados em blocos de 53 bits, atingindo velocidades a partir de 155 MB/s até 1,7Gb/s. Corresponde à futura tecnologia para redes de dados e permitirá, entre outras coisas, videoconferência em tempo real.

B2B - Business-to-Business expressão utilizada para definir as relações que acontecem entre empresas. Muitas vezes aparece como qualificativo de determinadas ações de marketing, geralmente o direto, cujo público alvo são empresas. As vendas para empresas são orientadas por estratégias bastante diversas daquelas que são usadas para atrair o consumidor. As chamadas para empresas geralmente são atendidas, mas nem sempre chegam até as pessoas que efetivamente respondem pelas decisões de compra. Discadores

preditivos raramente são usados para vendas telefônicas nas iniciativas Business-to-Business.

Backbone - A interconexão central de uma rede Internet. Pode ser entendido como uma espinha dorsal de conexões que interliga pontos distribuídos de uma rede, formando uma grande via por onde trafegam informações.

Baud rate - Medida de taxa de transmissão elétrica de dados em uma linha de comunicação. Mede o número de sinais elétricos transmitidos por unidade de tempo.

BBS - Bulletin Board System é um sistema que, tipicamente, oferece serviços de correio eletrônico, repositório de arquivos (de programas, dados ou imagens) e outros serviços tais como conversação on-line. Seus assinantes, usualmente, obtêm acesso através de linhas telefônicas (isto é, de voz) utilizadas via computador pessoal e modem.

BER – (Bit Error Rate) é um teste para determinar o percentual de bits errados em relação ao total de bits enviados, por exemplo, são transmitidos 1 milhão de bits por um canal e só um bit foi recebido com erro, então o nosso BER nesse canal de comunicações é de 10^{-6}. Uma fibra óptica tem um BER = 10^{-11} ou menor.

B-ISDN [RDSI-FL] – A B-ISDN (Broadband-Integrated Service Digital Network), ou seja, a Rede Digital de Serviços Integrados de Faixa-Larga é uma rede digital que integra serviços de diversas naturezas como voz, dados, imagens, etc. que deve substituir gradualmente a infraestrutura física atual das redes de telecomunicações, em que cada serviço tende a trafegar por segmentos independentes.

BIT – É a menor unidade de informação em um sistema binário, um estado zero ou um. O bit é a menor unidade de informação que um computador pode processar (usualmente indicado por 1 ou 0). 8 bits equivalem a um Byte (ou octeto). A palavra BIT resulta da contração das palavras em inglês **BI**nary digi**T** (BIT).

BITNET - Because It's Time Network. Rede de computadores formada em maio de 1981 para interconectar instituições educacionais e de pesquisa, fazendo uso de um protocolo chamado RSCS (Remote Spooling Communication System). Teve seu tráfego encerrado em 1996.

BNC - Vem de Baionet Nipple Conector, que poderia ser traduzido para "conector em forma de baioneta". É o conector usado em cabos de rede coaxiais, onde existe apenas um cabo de cobre, coberto por camadas de isolamento e blindagem.

BNC (2) - Um tipo de conector de vídeo encontrado em alguns monitores profissionais, onde existem cinco cabos separados, três para os sinais de cor (verde, azul e vermelho) e dois para os sinais de sincronismo horizontal e vertical. O objetivo de usar cabos separados é diminuir o nível de interferência, obtendo a melhor qualidade de imagem possível.

Bps - Uma medida da taxa de transferência real de dados de uma linha de comunicação. É dada em bits por segundo. Variantes ou derivativos importantes incluem Kbps (= 1.000 bps) e Mbps (= 1.000.000 bps).

BR Código ISO de identificação do Brasil na Rede, tipo de sufixo de um endereço na Internet. Um endereço brasileiro na Internet, registrado no órgão de gerenciamento da rede por aqui, sempre tem esta sigla.

Bridge - Um dispositivo que conecta duas ou mais redes de computadores transferindo, seletivamente, dados entre ambas.

Browser - Programa para visualizar, folhear páginas na Internet. Navegador, software para navegação da Internet. Os mais utilizado são o Netscape Navigator e o Internet Explorer.

Cabeamento estruturado - Técnica de disposição de cabos em um edifício caracterizada por uma configuração topológica flexível, facilitando a instalação e o remanejamento de redes locais.

Cabo UTP - Tipo de cabo mais utilizado nas topologias de redes de computadores atuais. É composto por quatro pares de cabos trançados entre si atingindo a velocidade de 155 milhões de bytes por segundo (155MBp/s). Pode alcançar até 100 metros entre duas conexões dentro da Categoria 5.

Categoria 5 - Categoria máxima homologada para redes de dados que estejam dentro das normas-padrão EIA/TIA (Associações das Indústrias Elétricas e Telefônicas dos E.U.A). Garantia de uma rede atual e com funcionamento perfeito.

CCITT - Acrônimo de Comitê Consultatif Internationale de Telegraphie et Telephonie, um órgão da International Telecommunications Union (ITU) das Nações Unidas que define padrões de telecomunicações. (Em 1993, foi extinto e suas atribuições passaram para o ITU-TSS, Telecommunications Standards Section da ITU.)

CERN - Trata-se do European Laboratory for Particle Physics, possivelmente o mais importante centro para pesquisas avançadas em física nuclear e de partículas, localizado em Genebra, Suíça. O nome CERN relaciona-se ao seu nome anterior, Conseil Europeen pour la Recherche Nucleaire. Para os usuários Internet, o CERN é conhecido como o local onde foi desenvolvido a Web.

Cliente - É um processo ou programa que requisita serviços a um servidor.

Ciberespaço - Espaço virtual onde a informação circula através de computadores. Espaço cibernético.

Conexão - Ligação entre computadores feita à distância que permite a comunicação de dados entre ambos.

Correio Eletrônico - Sistema de troca de mensagens através de redes de computadores. As mensagens podem conter textos e outros tipos de arquivos em anexo (attachment). Ver e-mail.

CPA - Central por programa armazenado. Centrais telefônicas com sistemas digitais controlados por computadores de alta capacidade de processamento, cujos terminais são os telefones.

Crosstalk - Tendência do sinal de um par de fios ser induzido em um par adjacente. D.G. Sigla para Distribuidor Geral. É um quadro que contém as conexões e organiza a distribuição de cabos de telefonia ou dados.

Domínio - É uma parte da hierarquia de nomes da Internet – DNS -, que permite identificar as instituições ou conjunto de instituições na rede. Sintaticamente, um nome de domínio da Internet consiste de uma sequência de nomes separados por pontos (.). Por exemplo, ci.rnp.br. Neste caso, dentro do domínio ci.rnp.br, o administrador do sistema pode criar diferentes grupos como info.ci.rnp.br ou staff.ci.rnp.br, conforme a necessidade.

Domínio público, (software de) - Programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso. Em geral, o software pode ser utilizado sem custos para fins estritamente educacionais e não tem garantia de manutenção ou atualização. Um dos grandes trunfos da Internet é a quantidade praticamente inesgotável de software de domínio público, de excelente qualidade, que circula pela rede.

Download - Ato de "baixar" e carregar um programa, ou seja, fazer a transferência de arquivos de um computador remoto para seu computador através da rede.

DNS - O Domain Name System (DNS) é um serviço e protocolo da família TCP/IP para o armazenamento e consulta a informações sobre recursos da rede. A implementação é distribuída entre diferentes servidores e trata principalmente da conversão de nomes Internet em seus números IPs correspondentes.

EDVAC - (Electronic Discrete Variable Automatic Computer) foi um dos primeiros computadores eletrônicos. Diferentemente de seu predecessor ENIAC, utilizava o sistema binário e possuía arquitetura de von Neumann.

ENIAC - (Electrical Numerical Integrator and Calculator) foi o primeiro computador digital eletrônico de grande escala. Criado em fevereiro de 1946 pelos cientistas norte-americanos John Eckert e John Mauchly, da Electronic Control Company. O ENIAC começou a ser desenvolvido em 1943 durante a II Guerra Mundial para computar trajetórias táticas que exigissem conhecimento substancial em matemática, mas só se tornou operacional após o final da guerra. O computador pesava 30 toneladas, media 5,50 m de altura e 25 m de comprimento e ocupava 180 m² de área construída. Foi construído sobre estruturas metálicas com 2,75 m de altura e contava com 70 mil resistores e 17.468 válvulas a vácuo ocupando a área de um ginásio desportivo. Segundo Tom Forester, quando acionado pela

primeira vez, o ENIAC consumiu tanta energia que as luzes de Filadélfia piscaram. Esta máquina não tinha sistema operacional e seu funcionamento era parecido com uma calculadora simples de hoje. O ENIAC, assim como uma calculadora, tinha de ser operado manualmente. A calculadora efetua os cálculos a partir das teclas pressionadas, fazendo interação direta com o hardware, como no ENIAC, no qual era preciso conectar fios, relês e sequências de chaves para que se determinasse a tarefa a ser executada. A cada tarefa diferente o processo deveria ser refeito. A resposta era dada por uma sequencia de lâmpadas.

EIA/TIA - Sigla para União das Associações das Indústrias de Telefonia e Associação das Indústrias de Elétrica dos Estados Unidos. Criaram as normas que regulam a instalação de redes de dados com o uso de cabos de par trançado (cabos UTP).

e-Accessibility - Basicamente o conceito de e-Accessibility é abrir a sociedade da informação para todos. Para se ter um sucesso real na Internet, os benefícios de uma sociedade da informação devem ser compartilhados com a sociedade toda, principalmente com aquelas pessoas que tem dificuldade no uso das novas tecnologias, tais como pessoas discapacitadas e as pessoas mais velhas ou idosas. Toda a sociedade deve ter as mesmas chances de poder usufruir os benefícios que traz a Internet, mas para isso as pessoas idosas e incapacitadas devem ter as ferramentas e as pessoas certas para lhes ensinarem o caminho de acessibilidade à Internet.

e-Competences - As mudanças, na sociedade da informação, vêm muito rápido: Novas tecnologias e serviços aparecendo a diário significam que os usuários devem estar preparados para atualizar suas habilidades e competências, aqueles que não o fizerem, devido a uma falta de oportunidade ou motivação, correm o sério risco de ficarem para traz. Portanto, é fundamental estar preparados para poder fazer uso destas novas ferramentas, isto se conhece como o e-Competences, isto é fundamental para ter as habilidades corretas, o conhecimento e a atitude para assim poder obter o melhor da atual sociedade da tecnologia e da informação. As novas tecnologias as quais podem fazer as nossas vidas e o nosso trabalho muito mais simples e fáceis estão sempre aparecendo no mercado, mas se as

pessoas não podem fazer um uso apropriado delas, correm o risco de ficar para traz na era da informação globalizada.

e-Mail - Do inglês, eletronic mail ou correio eletrônico. Endereço eletrônico para envio de mensagens na Internet. Exemplo: joaodasilva@embratel.com.br. Basicamente esta nomenclatura indica que o usuário João da Silva esta (ou tem) uma caixa de correio eletrônico no servidor da Embratel, a letra @ (arroba) é o comando "at" (dos sistemas UNIX) que traduzido significa algo assim como "em" ou "aonde", portanto, João da Silva se encontra em (at) um servidor da Embratel.

Ethernet - Padrão de rede (IEEE 802.3) local amplamente utilizado na década de 90, quando passaram a ser instalados em cabos UTP. É um sistema flexível, barato e com velocidade de transmissão de dados entre 4 e 10 MBp/s.

FAQ - Frequently Asked Questions, ou Perguntas Mais Frequentes. Perguntas e respostas das questões e dúvidas mais frequentes sobre um assunto.

FastEthernet - Padrão de rede local (IEEE 802.3u) do tipo Ethernet que atinge velocidades superiores daquelas encontradas nas velhas redes Ethernet (entre 80 e 100Mb/s).

FCS – O campo FCS (Frame Check Sequence), que traduzido do inglês seria algo assim como a sequência de verificação (checagem) do quadro, é extremamente útil para verificar que os dados enviados foram recebidos sem alterações durante a viagem desde o computador transmissor ao receptor que poderia estar na própria rede local ou uma rede remota. Nos quadros Ethernet o FCS é um campo de 4 Bytes que basicamente contem um algoritmo de controle de erros a nível de bit (Checksum) que permite revisar a integridade do quadro recebido, desta forma se o quadro esta correto ele é entregue às camadas superiores, caso contrário será descartado.

FDDI – O padrão FDDI (Fiber Distributed Data Interface) foi desenvolvido pelo ASC X3T9.5 da ANSI nos EUA e adotado pela ISO como padrão internacional (ISO 9314/1/2/3) em 1987. Inicialmente foi proposto para redes de comutação de pacotes, sendo mais tarde melhorado, onde a rede é dotada de capacidade de comutação de circuitos de modo a expandir o campo

de aplicações para a integração de voz, imagem e dados em tempo real. Este abrange o nível físico e de ligação de dados (as primeiras duas camadas do modelo OSI). A expansão de redes de âmbito mais estendido, ou seja, redes do tipo MAN (Metropolitan Area Network), são algumas das possibilidades do FDDI, tal como pode servir de base à interligação de redes locais, como em campus universitários. As redes FDDI adotam uma tecnologia de transmissão idêntica às das redes Token-Ring, mas utilizando cabos de fibra óptica, o que lhes concede capacidades de transmissão muito elevadas (na casa dos 100 Mbps ou mais) e a oportunidade de se alargarem a distâncias desde 100 até 200 Km, conectando entre 500 até 1000 estações de trabalho. Todas estas particularidades fazem do padrão FDDI altamente indicado para a interligação de redes LAN através de um backbone, neste caso, o backbone é a própria rede FDDI. Não existe requisito de configuração mínima. A rede FDDI fica altamente tolerante a falhas, devido à configuração de um anel duplo e por um mecanismo de isolação de falhas implementado nas estações.

FDMA – Os sistemas FDMA (Frequency Division Multiple Access) conhecidos como sistemas de acesso múltiplo por divisão de frequência são utilizados geralmente em sistemas de transmissão analógicos utilizando a multicanalização (ou multiplexação) em frequência. O funcionamento básico é o seguinte: Cada canal de voz (de vários), que originalmente ocupa o mesmo espectro de frequências com todos os outros canais, é alocado (através da multiplexação) a uma única banda de frequências, porem ocupando diferentes posições um atrás do outro (como um trem) e assim todo esse grupo de canais serializados podem ser enviados de forma simultânea por um único meio de transmissão. Desta forma podem se transmitir muitos canais de banda relativamente estreita, como por exemplo, canais de voz cada um com uma largura de 4 kHz, por um único sistema de transmissão de banda larga.

Fibra Óptica - Tipo de cabo feito de cristal de quartzo muito fino que permite o tráfego de grandes pacotes de informações em altíssima velocidade (2 bilhões de bits por segundo-2GBp/s) por meio de luz de 850 nanômetros de comprimento de onda, (multímodo) e que em geral é utilizado para a troca de pulsos informações entre grandes distâncias (aproximadamente 2.5 Km).

Frame-Relay - Protocolo que permite a conexão (com largura de banda ajustável de acordo com a demanda) entre duas redes locais através de uma rede pública utilizando comutação por pacotes.

Frequência - Medida pela qual uma corrente elétrica é alternada, em hertz.

FTP - File Transfer Protocol - Protocolo de transferência de arquivos, usado para enviar e receber arquivos via Internet.

Gateway - 1. Sistema que possibilita o intercâmbio de serviços entre redes com tecnologias completamente distintas, como FidoNet e Internet; 2. Sistema e convenções de interconexão entre duas redes de mesmo nível e idêntica tecnologia, mas sob administrações distintas. 3 Roteador (terminologia TCP/IP).

GIF - Graphic Interchange Format - Formato gráfico utilizado em imagens e com grande capacidade de compressão. A maioria das imagens animadas na Internet é feita nesse formato.

GNU - acrônimo recursivo de: GNU is Not Unix (em português: GNU não é Unix).

GPL - General Public License (Licença Pública Geral), GNU GPL ou simplesmente GPL, é a designação da licença para software livre idealizada por Richard Stallman no final da década de 1980, no âmbito do projecto GNU da Free Software Foundation (FSF). A GPL é a licença com maior utilização por parte de projectos de software livre, em grande parte devido à sua adoção para o Linux.

GUI – O termo corresponde à Interface Gráfica do Usuário, ou em inglês Graphic User Interface, é a consola gráfica que todo programa visual tem, onde é disponivilizada a interface para que o usuário possa interagir com um determinado aplicativo ou hardware do computador, tais como: botões, janelas, menus, etc.

Hacker - Indivíduos que elaboram e modificam software e hardware de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas. Originário do inglês, o termo é comumente utilizado no português sem modificação. Os Hackers utilizam toda a sua

inteligência para melhorar softwares de forma legal. Os Hackers geralmente são pessoas com alta capacidade mental e com pouca atividade social. Eles geralmente são de classe média e alta, com idade de 16 a 28 anos. A maioria dos Hackers são usuários avançados de Software Livre como o sistema operacional Linux. A verdadeira expressão para invasores de computadores é denominada Cracker e o termo designa programadores maliciosos e Ciberpiratas que agem com o intuito de violar, ilegal e/ou imoralmente,sistemas cibernéticos.

Hertz - Unidade de medida para definir frequência, em ciclos por segundo.

Hipertexto - Destaque de palavras, geralmente sublinhadas, em um texto que remete a outros locais (texto ou imagem ou site) permitindo uma leitura não linear.

Home Page - Primeira página de um site na Internet. Tornou-se sinônimo de endereço Web.

Host - Em português, hospedeiro. Computador que hospeda, guarda as informações para uma rede, no caso, a Internet.

HTML - HyperText Markup Language, linguagem de programação básica da Internet. Permite ao browser exibir textos e outros recursos multimídia de um site.

HTTP - HyperText Transfer Protocol - Protocolo ou padrão de transferência de arquivos HTML através da Internet.

HUB - Dispositivo de conexão eletrônica entre o servidor e os outros micros de uma rede do tipo Estrela. Podem ser passivos, apenas distribuindo o sinal; ativos, que possuem um repetidor que regenera o sinal, inteligentes, que permitem monitoração dos micros, ou chaveados que funcionam fechando conexões não utilizadas e acelerando a velocidade de transmissão.

Impedância - Oposição ao fluxo dinâmico corrente em um meio de transmissão.

Internet - Significa a "rede das redes". Originalmente criada nos EUA, que se tornou uma associação mundial de redes interligadas, que utilizam protocolos da família TCP/IP. A Internet provê transferência de arquivos, login remoto, correio eletrônico, news e outros

serviços. Uma coleção de redes locais e/ou de longa distância, interligadas numa rede virtual pelo uso de um protocolo que provê um espaço de endereçamento comum e roteamento.

Intranet - Rede particular usada em empresas e instituições. Utiliza a tecnologia do ambiente Web da Internet, porém com acesso restrito aos usuários desta rede privada.

IP - O Internet Protocol é o protocolo responsável pelo roteamento de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP, desenvolvida e usada na Internet. É considerado o mais importante dos protocolos em que a Internet é baseada.

IRC - Acrônimo de Internet Relay Chat, serviço que possibilita a comunicação escrita on-line entre vários usuários pela Internet. É a forma mais próxima do que seria uma “conversa escrita” na rede.

ISO - International Organization for Standardization (ISO), uma organização internacional formada por órgãos de diversos países que discute, especifica e propõe padrões para protocolos de redes. Muito conhecida por ter estabelecido um modelo de sete camadas que descreve a organização conceitual de protocolos, o OSI.

ITU - International Telecommunications Union. Órgão da ONU responsável pelo estabelecimento de normas e padrões em telecomunicações.

JAVA - Linguagem de programação criada pela Sun Microsystems. Permite baixar pequenos programas (Applets) que são ativados na própria máquina do usuário. Foi criada para poder ser utilizada em qualquer tipo de computador.

Jitter – É uma variação estatística do retardo na entrega de dados em uma rede, ou seja, pode ser definida como a medida de variação do atraso entre os pacotes sucessivos de dados. Observa-se ainda que, uma variação de atraso elevada produz uma recepção não regular dos pacotes. Logo, uma das formas de minimizar a variação de atraso é a utilização de buffer (memória), aonde esse buffer vai armazenando os dados à medida que eles chegam e os encaminham para a aplicação a uma mesma cadência. Minimizar o Jitter é de extrema importância nos serviços de Voz sobre IP (VoIP), por exemplo.

JPEG - Joint Photographic Experts Group - Formato de arquivo de imagens comprimidas.

kHz – Kilo-Hertz significa mil Hertz. O Hertz é a unidade de medida básica dos sinais periódicos em sistemas de telecomunicações por radiofrequência. Lembrar que um 1 Hertz = 1 ciclo por segundo, como os sinais são periódicos, por exemplo, um sinal de 10 kHz significa que ele cumpre 10 mil vezes seu período (ciclo) a cada segundo, em outras palavras, esse sinal gira a 10 mil ciclos por segundo. Outras medidas importantes nos sistemas de radiofrequência são os MHZ (Mega-Hertz), GHz (Giga-Hertz), THz (Tera-Hertz), etc.

LAN - Sigla para Rede de Área Local (Local Area Network), definida por uma rede de computadores restrita à uma mesma área, como por exemplo, um edifício comercial ou uma fábrica.

Largura de Banda - Capacidade de um determinado canal (fibra óptica, fio de cobre) de transmitir informações. No Brasil as linhas telefônicas convencionais utilizadas para transmissão de dados da Internet normalmente permitem uma largura de banda de 56 Kbps.

LINK - Ligação. Na Internet, uma palavra ou imagem em destaque que faz ligação com outra informação. Os links permitem a leitura não sequencial de um documento e são indicados nas páginas WEB pelo símbolo da mãozinha no lugar do cursor do mouse.

Login remoto - Acesso a um computador via rede para execução de comandos. Para todos os efeitos, o computador local, usado pelo usuário para "logar" no computador remoto, passa a operar como se fosse um terminal deste último.

Leased Line - Linha privada de telefonia utilizada por empresas para aumentar a segurança e velocidade de transmissão de dados.

MAN - Rede metropolitana é o acrônimo de Metropolitan Area Network, uma rede com tecnologia que opera a alta velocidade (de centenas de megabits por segundo a alguns gigabits por segundo) e que tem abrangência metropolitana.

MAU - Sigla para Unidade de Aceso de Mídia (Media Access Unit), dispositivo que serve como transceiver em uma rede do tipo Ethernet.

Mbps - Acrônimo para Mega bits por segundo, que é a medida da velocidade de transmissão de dados em um sistema, equivalente ao envio de um milhão de bits por segundo.

MHz (Mega Hertz) - Medida da freqüência de um sinal periódico que gira 1 milhão de ciclos por segundo. 1 MHz = 10^6 Hertz, ou seja, 1 milhão de Hertz. Normalmente utilizado para sinais de radio freqüência em telecomunicações ou na área de informática é utilizado como unidade de medida da freqüência de trabalho de um dispositivo de Hardware, por exemplo, para indicar a velocidade de processamento de um microprocessador.

MIMO - É o acrônimo em inglês para Multiple-Input Multiple-Output, ou seja, Múltiple Entrada Múltiple Saída. Esta sigla foi dada às antenas que fazem uso desta tecnologia em ambiente Wireless (sem fio). A tecnologia MIMO se refere especificamente à forma como são processadas (manejadas) as ondas de RF para transmissão e recepção nas antenas dos dispositivos Wireless como, por exemplo, nos roteadores em redes WLAN (Wireless LAN). A tecnologia MIMO aproveita os fenômenos físicos tais como a propagação multitrajeto (do sinal) para incrementar a taxa de transmissão e reduzir a taxa de erro. Em poucas palavras, a técnica MIMO aumenta a eficiência espectral de um sistema de comunicações Wireless através da utilização do domínio espacial, ou seja, muitas mais antenas e todas elas funcionando ao mesmo tempo. Com esta tecnologia é possível conseguir que cada uma das antenas possa receber ou transmitir de forma simultânea, para melhorar o desempenho do sistema. Além disso, pode corrigir de maneira muito mais eficiente as interferências, e conseguintemente, a qualidade do sinal recebido. Esta tecnologia foi implementada primeiramente em produtos com o padrão 802.11g, mas seu verdadeiro potencial foi atingido com os equipamentos utilizando o padrão 802.11n.

Modem - Sigla para Modulador/Demodulador (**Mod**ulator/**dem**odulator). Dispositivo que converte a informação digital em informação analógica para ser transmitida por uma linha telefônica da rede de comutação pública, e vice-versa.

Mosaic - Um programa cliente de fácil utilização projetado para procura de informações disponíveis na Web. Distribuído como freeware, o Mosaic foi criado pelo National Center for Supercomputing Applications (NCSA) dos EUA e tem capacidade multimídia.

Multicast - Um endereço Internet Classe D para um grupo específico de computadores em uma rede LAN, ou uma mensagem enviada a um grupo específico de computadores em rede. Um endereço Multicast é útil para aplicações como teleconferência.

NAT - Network Address Translation, é a técnica utilizada em redes de computadores, também conhecida como enmascaramento (masquerading) e consiste em reescrever os endereços IP de origem de um pacote que passam por um router ou firewall de maneira que um computador de uma rede interna tenha acesso ao exterior (rede pública).

Navegação - Ato de conectar-se a diferentes computadores da rede distribuídos pelo mundo, usando as facilidades providas por ferramentas como browsers Web. O navegante da rede realiza uma “viagem” virtual explorando o ciberespaço, da mesma forma que o astronauta explora o espaço sideral. Cunhado por analogia ao termo usado em Astronáutica.

Net - The Net ou a rede, normalmente é assim que se conhece atualmente a Internet.

Netiqueta - Um conjunto de regras de etiqueta para o uso socialmente responsável da Internet, ou seja, o modo como os usuários devem proceder na rede, especialmente na utilização de correio eletrônico.

Netnews - Usenet News, Usenet ou News. Serviço de discussão eletrônica sobre vasta gama de assuntos, cada qual ancorado por um grupo de discussão.

Newsgroup - Grupo temático de discussão do netnews.

NFS - O Network File System, desenvolvido pela Sun Microsystems Inc., é um protocolo que usa IP para permitir o compartilhamento de arquivos entre computadores.

NIC [CI] - Network Informations Center, centro de informação e assistência ao usuário da Internet que disponibiliza documentos, como RFCs, FAQs e FYIs, realiza treinamentos, etc.

NIS - Acrônimo para Network Information System (NIS), é um sistema distribuído de bases de dados que troca cópias de arquivos de configuração unindo a conveniência da replicação à facilidade de gerência centralizada. Servidores NIS gerenciam as cópias de arquivos de bases de dados, e clientes NIS requerem informação dos servidores ao invés de usar suas cópias locais destes arquivos. É muito usado por administradores UNIX para gerenciar bases de dados distribuídas através de uma rede.

NIS+ - Versão atualizada do NIS de propriedade da Sun Microsystems Inc. que provê mais recursos ao serviço e uma maior segurança.

Nó - Qualquer dispositivo, inclusive servidores e estações de trabalho, ligado a uma rede.

NOC [CO] - Network Operations Center. Um centro administrativo e técnico que é responsável por gerenciar os aspectos operacionais da rede, como o controle de acesso a mesma, roteamento, etc.

On-Line - Em linha. Você está on-line quando seu computador estiver conectado a outro computador ou a uma rede, permitindo a troca de informações através dessa conexão.

OSI - O Open Systems Interconnection (OSI) é um modelo conceitual de protocolo com sete camadas definido pela ISO, para a compreensão e o projeto de redes de computadores. Trata-se de uma padronização internacional para facilitar a comunicação entre computadores de diferentes fabricantes.

Pacote - Dado encapsulado para transmissão na rede. Um conjunto de bits compreendendo informação de controle, endereço fonte e destino dos nós envolvidos na transmissão.

Paridade - Método de checagem de erros na transmissão de informação por meio de bits.

Patch Panel - Dispositivo de conexão manual que permite uma fácil organização, e remanejamento dos pontos de um cabeamento estruturado, alterando a posição do ponto sem modificação física do cabo UTP.

Ping - O ping (Packet Internet Groper) é um programa usado para testar o alcance de uma rede, enviando a nós remotos uma requisição e esperando por uma resposta.

PIR [Ponto de Interconexão de Redes] - Locais previstos para a interconexão de redes de mesmo nível (peer networks), visando assegurar que o roteamento entre redes seja eficiente e organizado. No Brasil, os três principais PIR’s estão previstos em Brasília, Rio de Janeiro e São Paulo.

Plug-In - Programa adicional instalado em seu browser para ampliar seus recursos. Exemplos: Shockwave Flash, Real Audio, VDO e outros.

POP3 - O Post Office Protocol (versão 3) é um protocolo utilizado no acesso remoto a uma caixa de correio eletrônico. O POP3 está definido no RFC 1225 e permite que todas as mensagens contidas na caixa de correio eletrônico remota possam ser transferidas sequencialmente para o computador local. Desta forma, o usuário pode ler as mensagens recebidas, apagá-las, respondê-las, armazená-las, etc. Tudo localmente e Off-line.

Porta - Uma abstração usada pelo protocolo TCP/IP para distinguir entre conexões simultâneas para um único host destino. O termo também é usado para denominar um canal físico de entrada ou de um dispositivo.

PostMaster - E-mail do responsável pelo correio eletrônico de uma instituição.

PPP - Um dos protocolos mais conhecidos para acesso via interface serial, permite que um computador faça uso do TCP/IP através de uma linha telefônica convencional e um modem de alta velocidade. É considerado o sucessor do SLIP por ser mais confiável e eficiente.

PPPoE - (Point-to-Point Protocol over Ethernet) protocolo para conexão de usuários de uma rede Ethernet para a Internet. Seu uso é típico nas conexões de um ou múltiplos usuários em uma rede LAN à Internet através de uma linha DSL, de um dispositivo Wireless (sem-fio) ou de um modem de cabo broadband comum. O protocolo PPPoE deriva do protocolo PPP. O PPPoE estabelece a sessão e realiza a autenticação com o provedor de acesso a Internet.

Protocolo - Uma descrição formal de formatos de mensagem e das regras que dois computadores devem obedecer ao trocar mensagens. Um conjunto de regras padronizado que especifica o formato, a sincronização, o sequenciamento e a verificação de erros em comunicação de dados. O protocolo básico utilizado na Internet é o TCP/IP.

Provedor de Acesso - Instituição que se liga à Internet, via um ponto de presença ou outro provedor, para obter conectividade IP e repassá-la a outros indivíduos e instituições, em caráter comercial ou não.

Provedor de Informação - Instituição cuja finalidade principal é coletar, manter e/ou organizar informações on-line para acesso, através da Internet, por parte de assinantes da rede. Essas informações podem ser de acesso público incondicional, caracterizando assim um provedor não comercial ou, no outro extremo, constituir um serviço comercial onde existem tarifas ou assinaturas cobradas pelo provedor.

Provedor de Serviço - Pode ser tanto o provedor de acesso quanto o de informação.

RACK - Equipamento em forma de armário que armazena os diversos dispositivos de controle de rede (como Hubs, patch panels e D.I.O.s) que são encaixados como gavetas.

Rede - Conjunto de computadores interligados entre si e a um computador principal, o servidor. No caso da Internet, são vários servidores interligados em todo o mundo.

Repetidor - Um dispositivo que propaga (regenera e amplifica) sinais elétricos em uma conexão de dados, para estender o alcance da transmissão, sem fazer decisões de roteamento ou de seleção de pacotes.

RFC - Acrônimo para Request For Comments. RFCs constituem uma série de documentos editados desde 1969 e que descrevem aspectos relacionados com a Internet, como padrões, protocolos, serviços, recomendações operacionais, etc. Uma RFC é, em geral, muito densa do ponto de vista técnico.

Reply - Resposta dada a um e-mail recebido.

RJ-11 - Tipo de conector para telefonia em cabos UTP, de fácil manuseio e instalação.

RJ-45 - Tipo de conector para dados em cabos UTP de fácil manuseio e instalação.

Roteador - Dispositivo responsável pelo encaminhamento de pacotes de comunicação em uma rede ou entre redes. Tipicamente, uma instituição, ao se conectar à Internet, deverá

adquirir um roteador para conectar sua Rede Local (LAN) ao ponto de presença mais próximo.

Search - Busca, procura. Mecanismo de busca de informações na Internet. Cadê, Google e Yahoo são muito populares.

Servidor - Micro designado para gerenciar uma rede, organizando a transmissão de dados entre os computadores de uma empresa e para fora dela, além de armazenar bancos de dados e controlar o acesso de informações confidenciais. Uma rede pode ter mais de um servidor.

Shareware - Software distribuído gratuitamente por determinado período. Depois de um período inicial de testes, espera-se que o usuário envie um pagamento aos autores do programa para continuar a utilizá-lo.

Site - Espaço ou local de uma empresa ou instituição na Internet. Um site é composto de uma Home Page e várias outras páginas.

SLDD - Serviço por Linha Dedicada para Sinais Digitais, para interligação de dois, ou até cinco equipamentos de comunicação de dados.

SLIP - Serial Line IP é um protocolo Internet bastante popular usado via interfaces seriais.

Smiley - Uma "carinha" construída com caracteres ASCII e muito usada em mensagens eletrônicas para dar ideia de sentimentos ou emoções. Por exemplo, a mais comum é :-), que significa humor e ironia. Você deve girar o smiley 90 graus para a direita para entendê-lo.

SMTP - O Simple Mail Transfer Protocol é o protocolo TCP/IP usado para troca de mensagens via correio eletrônico na Internet.

SNMP - O Simple Network Management Protocol é um protocolo usado para monitorar e controlar serviços e dispositivos de uma rede TCP/IP. É o padrão adotado pela RNP para a gerência de sua rede.

Store-and-Forward - É o termo em inglês que significa Armazenar e Encaminhar (ou enviar) este método é muito utilizado nos sistemas por comutação de mensagens, onde toda a mensagem enviada pelo transmissor deve ser temporariamente armazenada em cada nó intermediário da rede, uma vez que a mensagem completa chegou para o primeiro nó de rede, esse nó deve enviá-la (ou encaminhá-la) para o seguinte nó e assim sucessivamente até a mensagem atingir seu destino final.

Switch - Dispositivo de rede que funciona como um distribuidor central da LAN e serve para segmentar uma rede em diferentes domínios de difusão (ou domínios de colisão). O Switch escuta em todos seus portos e constrói tabelas nas quais mapeia os endereços (físicos) MAC com o porto através do qual (um dado endereço MAC) pode ser alcançado. Desta maneira quando um computador (em um segmento da LAN) envia uma mensagem para outro computador (em outro segmento da LAN), a mensagem será lida pelo Switch e será encaminhada unicamente ao porto que contem o endereço MAC do computador destino assim limitando ao mínimo as colisões na rede LAN. Portanto, o Switch trabalha no nível 2 do modelo OSI.

TCP/IP - Transmission Control Protocol - Internet Protocol - Protocolo que define o processo de comunicação entre os computadores na Internet.

TDMA - Os sistemas TDMA (Time Division Multiple Access) conhecidos como sistemas de acesso múltiplo por divisão de tempo, são os sistemas de multiplexação (ou multicanalizaçao) mais utilizados na atualidade, especialmente nos sistemas de transmissão digital. Nestes sistemas a largura de banda total do meio de transmissão é designada a cada canal durante uma fração do tempo total (intervalo de tempo).

Telnet - Serviço que permite login remoto segundo o jargão e a vertente técnica Internet.

Token-Ring - as redes Token-Ring (IEEE 802.5) utilizam uma topologia lógica de anel. Quanto à topologia física, é utilizado um sistema de estrela parecido com o 10BaseT, onde temos Hubs inteligentes com 8 portas cada ligados entre si. Tanto os Hubs quanto as placas de rede e até mesmo os conectores dos cabos têm que ser próprios para redes Token-Ring.

Existem alguns Hubs combo, que podem ser utilizados tanto em redes Token-Ring quanto em redes Ethernet. A taxa de transferência de uma rede Token-Ring ia desde 4 até 16 Mbps.

Transceiver - Dispositivo que transmite e recebe informação de um computador para uma conexão de rede.

Transceiver Óptico - Dispositivo eletrônico que transforma sinais digitais provenientes de uma fibra óptica em sinais balanceados de 8 vias (RJ 45) para acoplamento de Hubs.

UNIX - É um sistema operacional portável, multitarefa e multiusuário originalmente criado por Ken Thompson, que trabalhava nos Laboratórios Bell (Bell Labs) da AT&T. A marca UNIX é uma propriedade do The Open Group, um consórcio formados por empresas de informática. Atualmente existem várias versões de sistemas UNIX que depende da arquitetura da máquina em questão, por exemplo, alguns dos Sistemas Operativos derivados do Unix são: BSD (FreeBSD, OpenBSD e NetBSD), Solaris anteriormente conhecido por SunOS (da Sun), IRIX (da Silicon Graphics), AIX (da IBM), HP-UX (da Hewlett-Packard), Tru64 (da Digital Equipment Corporation), Linux (nas suas centenas de distros para plataforma Intel x86/x64), e até o Mac OS X (baseado em um kernel Mach BSD chamado Darwin). Existem mais de quarenta sistemas operacionais *nix, rodando desde celulares a supercomputadores, de relógios de pulso a sistemas de grande porte.

Upgrade - Atualização de um software (versão mais recente) ou de um computador (configuração).

Upload - Transferência de arquivos de um computador para outro.

UDP - Acrônimo para User Datagram Protocol, o protocolo de transporte sem conexão da família TCP/IP, usado com aplicações como o de gerenciamento de redes (SNMP) e de serviço de nomes (DNS).

URL - Uniform Resource Locator - Sistema de endereçamento usado em toda a WWW. Exemplo: http://www.usp.br/

Vírus - Programa de computador feito para destruir outros programas ou arquivos específicos. Pode causar um prejuízo irreparável. O Anti-vírus é um programa que detecta e elimina os vírus.

VPN - É a sigla em inglês para denominar uma rede virtual privada (Virtual Private Network). Basicamente é uma conexão onde o acesso e a troca de dados somente é permitido a usuários e/ou redes que façam parte de uma mesma comunidade de interesse, por exemplo, uma empresa. Utilizando a técnica chamada de tunelamento, pacotes são transmitidos na rede pública, como por exemplo, pela Internet através de um túnel privado que simula uma conexão Ponto-a-Ponto.

Waffle - Um programa que possibilita a um BBS tornar-se um site Usenet.

WAIS - Acrônimo para Wide Area Information Server, é um serviço de bases de dados distribuídas acessíveis via Internet, cuja principal peculiaridade é a conversão automática de formatos para visualização remota de documentos e dados.

WAN - Sigla para Rede de Grande Área(Wide Area Network), definida por uma rede de computadores ligada por meios de comunicação de longa distância, como por exemplo, sinais de rádio, L.P.s (linhas privadas) e até mesmo satélites.

Webmail - Interface via web que permite ao usuário ler e processar seus e-mails diretamente de uma página na internet. Ele tem todas as características de um programa de e-mail, possibilitando que você leia uma nova mensagem, envie e/ou encaminhe mensagens, envie e/ou veja anexos, podendo, inclusive, usar pastas para organizá-las.

Webtrends - Solução de Análise e Gerenciamento Web que fornece dados estatísticos de todos os elementos sobre a atividade do visitante no site, possibilitando, assim, melhorias sobre performance, disponibilidade e resultados esperados.

WHOIS - Banco de dados de informações sobre domínios, redes, hosts e pessoas, fornecendo um serviço de diretório de usuários da Internet.

Wi-Fi - Wireless Fidelity. É a tecnologia de interconectividade entre dispositivos sem o uso de fios. É disponibilizado através de um determinado ponto (Hotspot) que cobre uma faixa de frequência e estabelece dentro desta faixa o acesso para uma conexão de Internet.

WiMAX - (Worldwide Interoperability for Microwave Access/Interoperabilidade Mundial para Acesso de Micro-ondas) Especifica uma interface sem-fio para redes metropolitanas (WMAN) de conexão de banda larga (last mile) oferecendo conectividade para uso doméstico, empresarial e em hotspots. O benefício crucial do padrão WiMAX é a oferta de conexão internet banda larga em regiões onde não existe infraestrutura de cabeamento telefônico ou de TV a cabo.

Wireless - A tecnologia Wireless (sem-fios) permite a conexão entre diferentes pontos sem a necessidade do uso de cabos telefônico, coaxial ou óptico, por meio de equipamentos que usam radiofrequência (comunicação via ondas de rádio) ou comunicação via infravermelho, como em dispositivos compatíveis com IrDA. Wireless é uma tecnologia capaz de unir terminais eletrônicos, geralmente computadores, entre si devido às ondas de rádio ou infravermelho, sem necessidade de utilizar cabos de conexão entre eles. O uso da tecnologia Wireless vai desde transceptores de rádio como walkie-talkies até satélites artificiais no espaço. Seu uso mais comum é em redes de computadores, onde a grande maioria dos usuários utiliza-se da mesma para navegar pela Internet no escritório, em um bar, um aeroporto, um parque, em casa, etc. Uma rede de computadores sem-fios são redes que utilizam ondas eletromagnéticas ao invés de cabos, tendo sua classificação baseada na área de abrangência delas: redes pessoais ou curta distância (WPAN), redes locais (WLAN), redes metropolitanas (WMAN) e redes geograficamente distribuídas ou de longa distância (WWAN).

WORM - Acrônimo de Write Once Read Many. 1. Ferramenta de busca na rede Web; 2. Verme, programa que, explorando deficiências de segurança de hosts, logrou propagar-se de forma autônoma na Internet na década de 80.

WWW - World Wide Web. É a área multimídia da Internet. Por ser a mais popular é confundida com a própria Internet. Além da WWW existem outras áreas da Internet, como: FTP, Gopher, Usenet e Telnet.

BIBLIOGRAFIA

KUROSE, James F.; Ross, Keith W. – Redes de Computadores e a Internet - Uma Abordagem Top-down – 5a Edição. / Pearson Education – Br

STALLINGS, William – Data and Computers Communications. New Jersey. Prentice-Hall Inc. Fifth Edition, 1997.

COMER, Douglas, E. – Computer Networks and Internets. New Jersey. Prentice-Hall Inc., 1997.

TANENBAUM, Andrews. Redes de computadores 4a Edição. Rio de Janeiro Campus, 2003.

TORRES, Gabriel. Redes de Computadores Curso Completo. Rio de Janeiro, Axcel Books, 2001.

SASSER, Susan B. Instalando a sua própria rede. São Paulo, Makron Books, 1996.

SOUSA, Lindeberg Barros de. Redes de Computadores: Dados, Voz e Imagem. São Paulo, Érica, 1999.

MORAES, Alexandre Fernandes de, Cirone, Antônio Carlos. - Redes de Computadores da Ethernet à Internet - São Paulo. Érica, 2003.

CARDOSO, Carlos, Gutierrez, Marcos Antônio – Redes Curso Básico e Rápido. Rio de Janeiro. Axcel Books, 2000.

MARIMOTO, Carlos Eduardo, Redes - Guia Prático / Sul Editores

BENEDETTI Ryan, Anderson, Al; Redes de Computadores / Alta Books

Links:

http://www.hdtechnology.com.br/

http://www.recitronic.com.br/

http://www.clubedohardware.com.br/

http://www.guiadohardware.net/index.php

http://www.redes.usp.br/

http://www.projetoderedes.com.br/

http://www.networkexperts.com.br/

http://www.teleco.com.br/

http://www.dicas-l.com.br/

http://www.mobilezone.com.br/

http://www.microsoft.com/pt/br